CISO MAG

beyond cybersecurity

Volume 5 | Issue 06 | June 2021

"Public GitHub is often a blind spot in the security team's perimeter"

Jérémy Thomas
Co-founder and CEO
GitGuardian

54

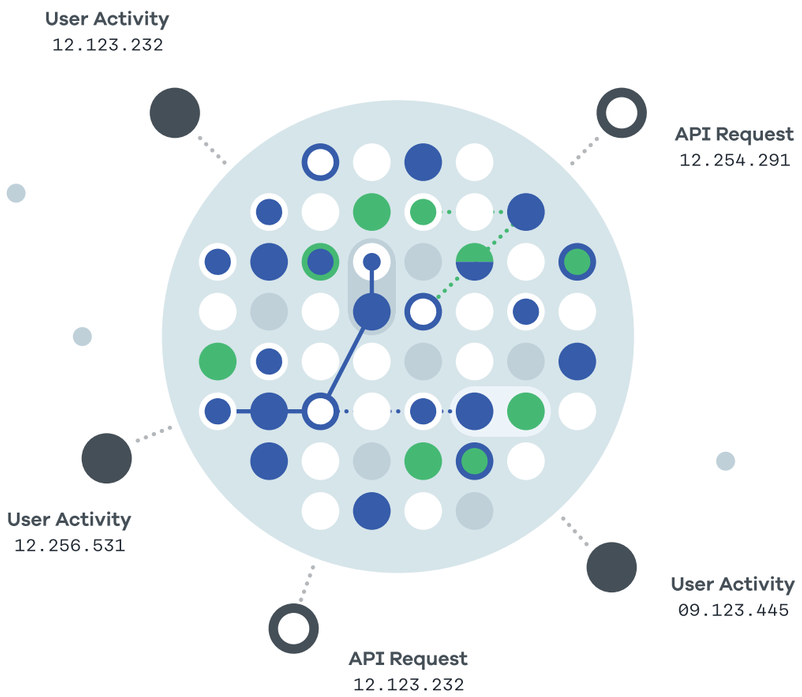
UNDER THE SPOTLIGHT

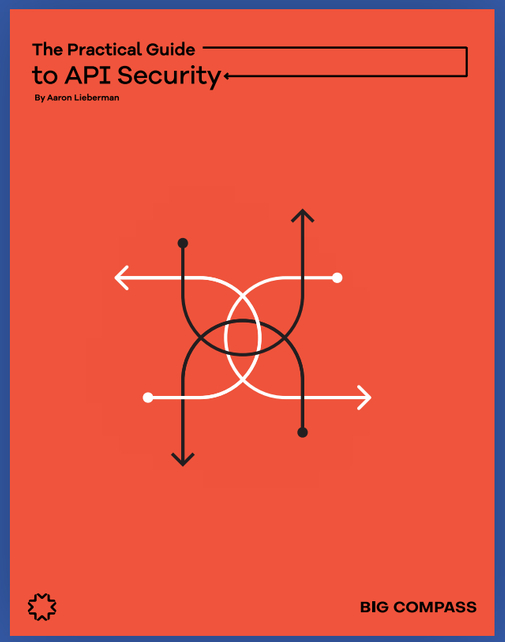
IMPLEMENTING DIGITAL FORENSICS IN EMERGING TECHNOLOGIES

TRACEABLE_

Traceable enables security to manage their application and API risks given the continuous pace of change and modern threats to applications.

Know your application DNA





Download the practical guide to API Security

Learn how to secure your API's. This practical guide shares best practices and insights into API security. **Scan or visit Traceable.ai/CISOMag**

TRACEABLE_

CISO MAG
beyond cybersecurity

Volume 5 | Issue 06
June 2021

President & CEO
Jay Bavisi

Editorial
Editor-in-Chief
Brian Pereira*
brian.p@eccouncil.org

Assistant Editor
Augustin Kurian
augustin.k@eccouncil.org

Sr. Feature Writer
Rudra Srinivas
rudra.s@eccouncil.org

Sr. Technical Writer
Mihir Bagwe
mihir.b@eccouncil.org

Sub Editor
Pooja Tikekar
pooja.v@eccouncil.org

Management
Senior Vice President
Karan Henrik
karan.henrik@eccouncil.org

Director of Marketing
Nandakishore
nandakishore.p@eccouncil.org

General Manager - Marketing
Seema Bhatia
seema.b@eccouncil.org

Senior Director
Raj Kumar Vishwakarma
rajkumar@eccouncil.org

Head - Research & Content
Jyoti Punjabi
jyoti.punjabi@eccouncil.org

Publishing Sales Manager
Taruna Bose
taruna.b@eccouncil.org

Manager - Digital Marketing
Rajashakher Intha
rajashakher.i@eccouncil.org

Asst. Manager Visualizer cum Graphic Designer
Jeevana Rao Jinaga
jeevana.r@eccouncil.org

Manager – Marketing and Operations
Munazza Khan
munazza.k@eccouncil.org

Image credits: Shutterstock & Freepik
Illustrations, Survey Design, Cover & Layouts by: Jeevana Rao Jinaga

EDITOR'S NOTE

DIGITAL FORENSICS EDUCATION MUST KEEP UP WITH EMERGING TECHNOLOGIES

Brian Pereira
Editor-in-Chief

"There is nothing like first-hand evidence."
- Sherlock Holmes

If the brilliant detective **Sherlock Holmes** and his dependable and trustworthy assistant **Dr. Watson** were alive and practicing today, they would have to contend with crime in the digital world. They would be up against cybercriminals working across borders who use sophisticated obfuscation and stealth techniques. That would make their endeavor to collect artefacts and first-hand evidence so much more difficult!

As personal computers became popular in the 1980s, criminals started using PCs for crime. Records of their nefarious activities were stored on hard disks and floppy disks. Tech-savvy criminals used computers to perform forgery, money laundering, or data theft. Computer Forensics Science emerged as a practice to investigate and extract evidence from personal computers and associated media like floppy disk, hard disk, and CD-ROM. This digital evidence could be used in court to support cases.

Until then, forensics was straightforward. Investigators had to locate the media and extract the data. They ran into a wall if the files were password protected or encrypted, but experts soon found a way around that challenge.

Then computers were connected to the networks, and eventually to the Internet. And the trail got longer and ran into a maze. So, we had a new branch, Network Forensics.

As technology evolved through the years, cybercrime extended to the Web, the cloud, and mobile devices. Malware became more sophisticated, and today we have ransomware.

Smartphones with watertight encryption came along, and that posed a huge challenge to forensics investigators. Do you remember the Apple iPhone incident a few years ago, when the FBI asked Apple to unlock the iPhone of a criminal? Apple refused. The tussle between the FBI and Apple was holding up the investigation until a third-party finally figured out how to unlock the iPhone.

Today, forensic experts travel to different countries to find digital evidence, as cybercrime is performed across borders. These digital forensic experts are the modern-day version of Holmes investigating clues left by criminals.

Emerging technologies and borderless cybercrime have made Digital Forensics more challenging than ever.

So how do we counter all this with a completely different strategy?

SURVEY & REPORT

To better understand the challenges and state of readiness in implementing Digital Forensics in emerging technologies, ***CISO MAG,*** in collaboration with EC-Council's CHFI group (Computer Hacking and Forensic Investigation), launched a Technology Trends Survey in April 2021. The resulting report included in this issue offers an in-depth analysis of how important it is to incorporate the effects of digital forensics on emerging technologies into the curriculum of digital forensic education.

The **key findings** of the **survey,** as well as the insights provided by experts in our **Focus on Forensics** section, will be an eyeopener for those seeking training and a career in Digital Forensics.

And it surely is a career with a lot of opportunities!

INDEX

Contents

Is Forensics Possible in a COVID-19 scenario?

Narendra Sahoo
Founder and Director
VISTA InfoSec

The COVID-19 pandemic has created havoc not just in the lives of people but also rocked the business world globally. With countries going into lockdown, businesses are today forced to adapt to the situation and operate remotely. With this, businesses are confronted with new challenges and threats. Although organizations around the globe have adopted the work-from-home operating model, this has opened doors to malicious cyberattacks. With the new working norms and companies accelerating their digital transformation, cybersecurity is now a major concern.

While the entire world is focusing on health, the economy, and restoring normalcy, criminals are constantly capitalizing on the situation to stage a well-planned cyberattack. Not only does the incident of cyberattack have severe reputational, legal, operational, and compliance implications, it also severely impacts the forensic investigation. Speaking more on this, we have explained in the article the challenges of remote working, pre-requisites to prevent incidents of the breach, the protocols to be followed in case of a data breach, and all the nitty-gritty of cyber forensics. The article provides insight on the impact of remote working on Cybersecurity, and the process of cyber forensics in case of a breach.

What happens in Cyber Forensics?

Handling a data breach incident in a normal scenario is very different from the current situation for both the organization and the cyber forensic team. Before the pandemic, when businesses were running in a controlled environment, even in case of a data breach, immediate response, measures to contain, and investigations helped lower the impact. However, now in the pandemic situation, with the remote working model, the situation is completely different. Not only has this increased the risk of a cyberattack, but it has also hampered the process of investigation and containing the situation in case of a data breach. But, before we get into the details of the challenges faced in cyber forensics during the pandemic, let us first understand the process of a cyber forensics investigation.

Cyber Forensics Investigation

Before the pandemic, when a data breach incident occurred, organizations had to follow a specific protocol to respond and contain the incident. With that, a cyber forensic team investigates the situation at the location and helps the organization respond, recover and resolve the incident. The process of handling the incident involves two primary steps which include:

- Responding and Containing Incidents
- Investigating the Incident and Collecting Evidence

While the approach taken by the organization may vary based on their priorities, severity of the incident, and impact of the incident, there are certain basic protocols organizations must follow. Given below is a list of protocols that organizations should follow in case of a data breach. Once there is a breach, the organization should follow a few essential steps immediately to limit the impact of the breach.

Protocol to be followed in a Data Breach Incident

Step 1: Survey the damage

Once the organization discovers the data breach incident, the Information Security Officer along with the designated information security team should conduct an internal investigation. This is to first determine whether an incident has happened and to access the impact of the incident on critical business functions. They further need to conduct an in-depth investigation to identify the attacker/source of the attack, discover the exploited security vulnerabilities, identify immediate steps that can be taken to limit the loss, and determine steps for resolution and improvements. If an attack is confirmed, it is well advised to hire external professionals to investigate and take steps.

Step 2: Contain the Situation

Once the organization determines the impact of the incident, security vulnerabilities, and the attackers they should take steps to contain the damage. This should include steps like:

- Isolating the compromised network
- Filter or block traffic
- Re-route network traffic
- Temporarily disable remote access capability and wireless access points (situation-based)

- Change Access Control credentials
- Segregate all hardware devices from the infected system or network
- Isolate and quarantine identified malware rather than deleting it (for future analysis and evidence)
- Preserve firewall settings, firewall logs, system logs, and security logs for future analysis and evidence

Step 3: Record and file details

Once the survey is conducted and situations are contained, the information security team must maintain a written log of all the actions taken to respond to the breach. The information that should be collected and filed must include:

- Details of the affected systems
- Compromised network and accounts
- Services disrupted due to the breach
- Data and network affected by the breach
- Amount and type of damage done to the systems

Other details that should be documented must include details like how you learned about the breach, the date, and time you were notified, how were you notified, all actions taken between now and the end of the incident, date and time you isolated systems infected, and disconnected from the Internet, disabled remote access, changed credentials/passwords, and system hardening or any other remediation steps taken over time.

Step 4: Inform the Regulators

In case of a breach, the organization should immediately report the incident to law enforcement or regulators. The notifiable breach should be reported at the earliest but not later than 72 hours after being aware of the breach. The duration depends primarily on the local regulatory framework, compliance requirements, and client SLA. Reporting should be done only by approved official channels and personnel. All other personnel should be explicitly prevented from sharing any information with anyone, whether internal or external to the organization.

When reporting the incident of the breach, the organization will have to provide the following details to the regulator:

- Description of the nature of data breach
- Approximate number of individuals affected
- Nature of the data which is breached
- Name and contact details of the Data Protection Officer
- Severity of the data breach
- Description of measures taken to contain the impact and handle the data breach

In case the data breach involves a large number of people affected, then the regulator may contact the media.

Step 5: Inform those affected

Individuals affected by the incident of breach must be informed and notified about the risk. The individuals may be notified via phone, email, or in person. However, the information provided to them will be restricted to avoid unauthorized disclosure. When notifying the incident to individuals, the organization will have to provide the following details in clear and plain language:

- Nature of the data breached
- Name and contact details of the Data Protection Officer
- Description of the likely consequences of the data breach
- Description of measures taken and actions that may be implemented to deal with the breach
- Description of the measures taken to mitigate any possible adverse effects
- Give specific and clear advice on steps to be taken to protect themselves
- Mention the kind of assistance you may offer them to take any specific measures

Step 6: Analyze the Breach Incident

A data breach can greatly impact the organization in terms of reputational loss, monetary loss, and other legal implications. So, with such a bitter experience, the organization must analyze and take note of the incident to establish a strong cybersecurity defense and Incident Management Response. This will enable them to take preventive measures in the future and further enable them to handle the incident better. The organization must analyze the incident by:

- Documenting all the mistakes
- Assess the mistakes and listing out preventive measures for the future
- Design a training program and incorporate lessons learned in the program

COVID-19 and Cyber Forensics Challenges

As we know, the COVID-19 pandemic has pushed companies to operate remotely and adapt to the new working style for most businesses.

This has severely affected the cybersecurity measures and initiatives of organizations that otherwise work as a strong defense against any cyberthreats. Moreover, in the current scenario when the breach occurs, the cyber forensic team faces exasperating challenges that severely hamper the investigative process. Listed below are some of the challenges that the forensic team faces in the current scenario that makes the investigation process extremely difficult:

- **Investigating the environment -** Under normal circumstances, the investigation is a lot easier for it is performed in a controlled environment using well configured and company-approved hardware/software. However, in a remote working scenario, with systems and networks operating in a neutral and publicly accessible environment, it makes the investigation challenging. Moreover, identifying the attacker, discovering the exploited security vulnerabilities, and determining the systems and networks compromised can be very difficult.
- **Containing situations –** This can be very challenging during the pandemic as the entire office is running remotely. Taking preventive measures like isolating the network, changing access control credentials, dealing with service disruption, and ensuring Business Continuity becomes a nightmare.
- **Evidence Gathering –** It is extremely difficult for the organization and the forensics team to prevent contamination of evidence. The isolation and collection of evidence is a crucial part of investigation for which ensuring the preservation of trails is essential. However, in situations like these, there is a high probability of evidence contamination or destruction, especially in an uncontrolled environment where it is difficult for the team to track down the trail of incidents.
- **Actionable Measures -** Taking decisive and actionable measures can also be a task in this scenario. With no trail of evidence, or identification of attacker, the exploited security vulnerabilities, or the systems and networks compromised, taking any decisions or implementing any action can be difficult. For instance, without identifying the exploited security vulnerabilities or the systems and networks compromised, isolating the compromised network or filtering, blocking or re-routing of network traffic can be a huge challenge.

With challenges like these, the organization and the forensics team will be in no position to perform or close an investigation. However, if organizations come up with a process to deal with situations like these and train their staff accordingly, things can probably be a lot easier. Ideally, organizations must conduct training programs for staff to deal with such situations. Moreover, conducting regular awareness programs on prevailing threats will also alert the staff about the potential threats they may encounter with time. We also believe that having in place strong security measures, designed for the work-from-home model will give the organization an edge in the prevailing situation.

Here is a summary of pre-requisites that organizations must follow and have in place to prevent incidents of a breach.

Pre-requisites to prevent incidents

In this new environment and working model, the organization and its internal Cybersecurity team must be proactive in implementing measures and monitoring crucial systems and data. Constant vigilance and aggressive confrontation of potential risks are the need of the hour. Having said that, here are some measures that can help businesses deal with the prevailing situation:

Work-from-home Policy

Create a work-from-home policy that includes all the guidelines that staff members working remotely need to follow. It should outline necessary steps that need to be taken on ways to access systems, data restricted from sharing, and other related details. Establishing a proper policy will eliminate more than half of your cybersecurity problems. Moreover, remote workers will know the guidelines and practice their work process accordingly, to meet the requirements and working standards of remote cybersecurity.

Awareness programs

For starters, the organization should educate its staff members working from home about various scams, phishing techniques that are flooding the market and threatening the security of IT infrastructure. They should be trained to avoid becoming victims of such scams. E-learning or web-based training programs can be a good solution.

Cloud Security

Organizations should be swift with deploying technologies and solutions that are effective and quick to deploy. For instance, considering the adoption of a cloud-based solution. Further, implementing strong cloud-based security and platform services will ensure safe business operations. This initiative adds additional layers of protection and enhances the layers of security. With cloud-based security, the internal IT security team can also manage and monitor systems remotely.

For instance, the cloud-based secure virtual desktop services provide IT professionals with remote access to employee's systems, including files and networks. Further, deployment of Cloud-based data leakage prevention and threat-protection controls can secure critical assets. Moreover, the cloud-based managed detection and response technology can be extended to remote workplaces.

VPN Set-up

One way of ensuring good security is using a Virtual Private Network (VPN). VPN allows a secure connection by providing an alternative IP address to your network while bringing in traffic to your network. It provides security by protecting the browsing activity from hackers and scammers on public Wi-Fi. It also helps bypass geographic restrictions on websites or even streaming audio and video. The technology helps hide your private information and even prevents data-throttling. Moreover, VPN encrypts data transfer thus ensuring data protection.

PAM

Organizations can also use Privileged Access Management (PAM) services to allow special remote access to their IT and application administrators. With multi-factor authentication including biometric and text-based methods, it can enable security on risk-based access to internal applications that are accessed remotely.

Encrypted communication tools

When working remotely, employees must use encrypted commination tools to prevent any security issues. Communication tools include emails, video conferencing, and data transfer that may involve the use of sensitive data. So, using encrypted tools for remote working can prevent data security issues.

Conclusion

In the prevailing pandemic situation, remote working will now be the new norm for most organizations around the globe. With that said, the cybersecurity program should be made the top focus point for all businesses. While cyber forensic investigation can still be a huge challenge, establishing strong cybersecurity measures should be the top priority. Taking necessary preventive measures is essential for businesses to prevent any incidents of the breach.

Although tackling the implications of remote working on cybersecurity can be complicated and will require legislative intervention, yet on the business level, it can be dealt with, by implementing necessary security measures. Businesses must consider allocating resources to IT Infrastructure and cybersecurity for improved cybersecurity, better-integrated, and well-encrypted communications, automation, and enhanced IT management. This is for building a stringent cybersecurity defense mechanism.

About the Author

Narendra Sahoo (PCI QSA, PCI QPA, CISSP, CISA, and CRISC) is the Founder and Director of VISTA InfoSec, a global Information Security Consulting firm, based in the U.S., Singapore & India. Mr. Sahoo holds more than 25 years of experience in the IT Industry, with expertise in Information Risk Consulting, Assessment, and Compliance services. VISTA InfoSec specializes in Information Security audit, consulting, and certification services which include GDPR Compliance and Audit, HIPAA, CCPA, NESA, MAS-TRM, PCI DSS Compliance & Audit, PCI PIN, SOC2, PDPA, PDPB to name a few. The company has for years (since 2004) worked with organizations across the globe to address the Regulatory and Information Security challenges in their industry. VISTA InfoSec has been instrumental in helping top multinational companies achieve compliance and secure their IT infrastructure.

How Digital Forensics Complements Cybersecurity

Anis Pankhania
CISO
Cloud Infrastructure Services,
Capgemini India

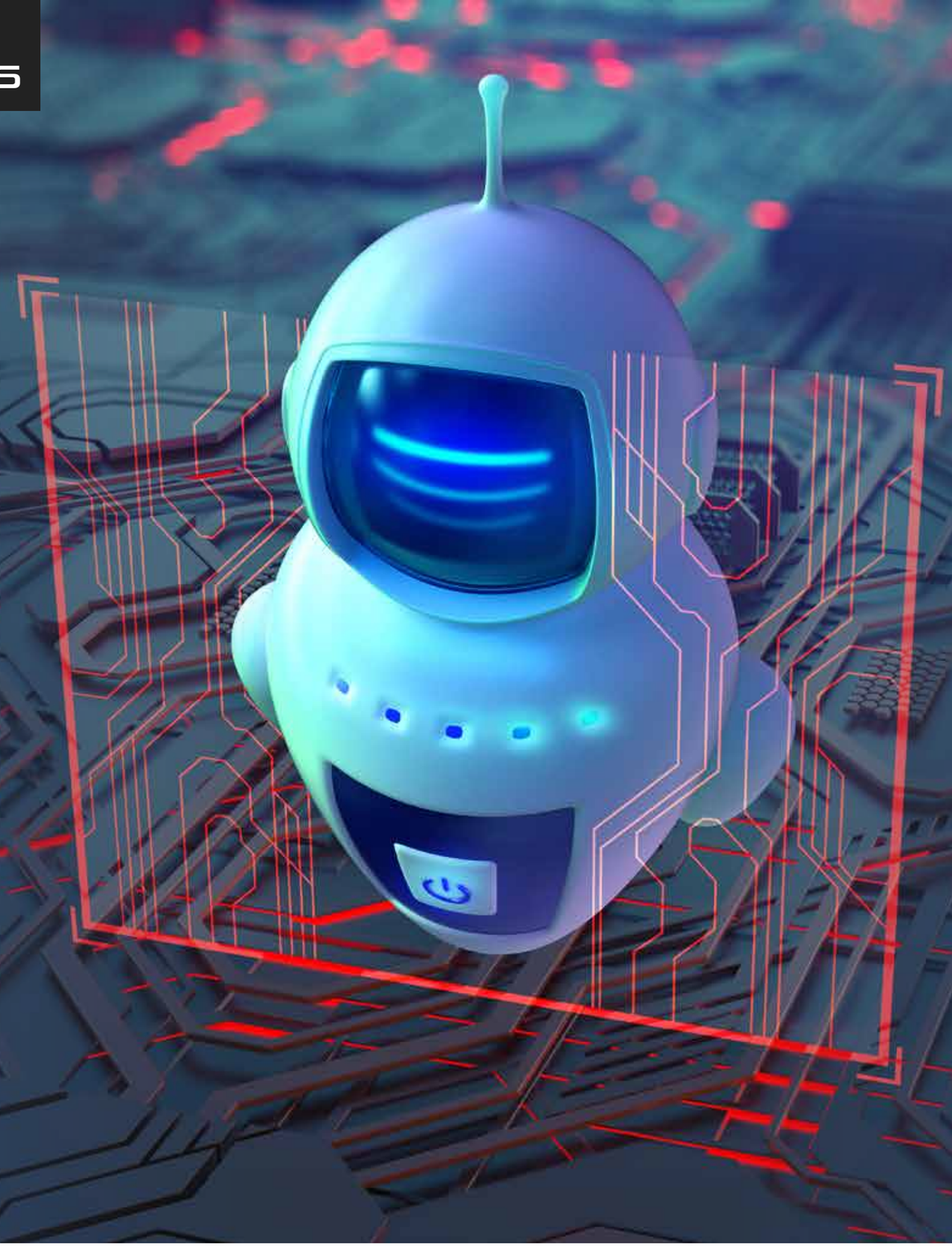
Analyzing pieces of evidence found in a digital device is a laborious task. The challenges of which are further augmented by the ever-changing methods and technologies adopted by threat actors. Cyber forensics applies scientific methods to analyze and recreate the sequence of events that occurred either during the security breach in a corporate firm or during a criminal investigation for the law and enforcement body. This process of procuring artifacts, analyzing, documenting, and reporting is accompanied by many challenges and aided by useful tools and technology that this article aims to describe in brief.

Trends in Cybercrime

As stated earlier, the ever-changing threat landscape and the development technology being used maliciously pose a variety of challenges for the digital forensic investigator. Organizations are under constant threat of attack as there is no shortage of factors that induce disruption, which range from substantial information breaches to malware and botnet assaults. Some of the current trends in cyberattacks could be listed as:

- **Malware:** The spreading of malware today has turned into a sort of continuous campaign, with the majority of recent incidents involving the use of ransomware or some other form of malware. Spyware and ransomware are the most dangerous malware that poses a serious threat to information security, as they tend to encrypt or exfiltrate sensitive information. To make matters worse, this malware is increasingly equipped with sophisticated anti-forensic techniques that tend to increase the amount of time required for the investigators to retrieve any artifact or evidence. Encryption of data itself is an anti-forensic technique wherein if the threat actor gains a greater privilege, then not only the sensitive information (which is to be held for ransom) but also their digital footprints could be encrypted, never to be decrypted again. Ransomware typically targets all types of file extensions without any barriers, as such files that are of some importance to the victim. Even if the targeted organization pays the ransom, which by the way is now illegal, according to the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), there is very little probability of getting back the encrypted data.
- **Botnets:** Botnets are compromised systems that are controlled by the threat actors through a remote network of command and control without the knowledge of their owners/users. Botnets are generally used to conduct a DDoS attack, cryptojacking, click fraud, phishing, spam, and multiple other malicious operations. The threat actor could issue the command for the attack to the bots at any moment through the command-and-control network. A high-level of internet privacy and security knowledge is required on the part of the network administrator and forensic analyst to identify and stop the botnet attack.
- **Cryptojacking:** This is the advanced application of the botnet network, where the bots are installed with crypto mining programs to mine cryptocurrency. This cryptojacking malware is designed to hijack the processor of the device to run crypto-mining programs effectively, which will, in turn, overheat the power source, hence, damaging the device. Though crypto mining is not illegal, it is a legitimate method used by blockchain experts to mine and generate digital currency, but this process requires high and fast performance on the part of the systems, which is generally expensive. Where legitimate miners use their high-end systems and tools, malicious attackers use their botnet network to mine digital currency.

FOCUS ON DIGITAL FORENSICS



Importance of Cyber Forensics

Though it may seem that cyber forensics exists due to the existence and implementation of cybersecurity programs, and a failed information security framework feeds the digital forensics operations. But in reality, both are co-dependent and go hand-in-hand. Digital forensics provides the information that feeds the developments in cybersecurity. The cumulative information about the state of security is obtained through numerous cases investigated through cyber forensics. Understanding this delicate balance between the two will help cybersecurity professionals to create a better security architecture. To state this plainly, the two main uses of implementing cyber forensics are:

- **Preventing attacks:** Digital forensics analyzes the crime scene in the digital landscape and obtains information upon which the cybersecurity industry could build better security solutions to patch the vulnerabilities and prevent malicious hackers from accessing the information on a network, website, or device. Threat actors are skilled at identifying and exploiting vulnerabilities of a system or application. Hence, digital forensics is important to study in detail the tactics used by the attacker and provide information to security personnel to develop countermeasures.
- **Data recovery:** The main aim of any cyber forensic investigation is recovering the deleted or damaged information. This is generally how digital forensics is understood in corporate and IT sectors. Digital forensics recovers information using complex tools and techniques in business data breaches or a civilian data breach. The recovered data could either be used as evidence in a court of law or to help the victim restore business continuity. This aspect of cyber forensics extends into the disaster recovery model of the information security framework, where the plan involving a step-by-step strategic approach is designed and implemented to recover disrupted networks in case of both cyberattack or natural disaster.

Digital Forensic Tools

There exist several tools to aid the cyber forensic process, which are available in both open source and commercial modes. The wide scope of digital forensic investigation requires a combination of different tools and suites working together to find evidence and recover data. Some of the major tools and suites are listed below as follows:

- **Autopsy:** The most widely known tool for forensic investigation is a GUI-based tool that analyzes hard drives and mobile devices. Its prime feature involves timeline analysis, hash filtering, keyword search, web artifacts extraction (history, bookmarks, and cookies), data carving (PhotoRec), multimedia extractors, and IoC collection (Indicators of Compromise - STIX).
- **CAINE:** The Computer-Aided Investigative Environment (CAINE) is a user-friendly interface that has an optimized environment to conduct a forensic analysis, which also includes a semi-automatic report generator.

FOCUS ON DIGITAL FORENSICS

- **Encrypted Disk Detector:** MAGNET's Encrypted Disk Detector is a command-line tool that can search for encrypted data on the physical drives of a system.
- **Magnet RAM Capture:** As the name suggests, it is used to capture volatile data on the physical memory, allowing forensic investigators to recover important information. It captures and exports the memory information in Raw (.DMP/.RAW/.BIN) format and works with other Magnet AXIOM and Magnet IEF tools to analyze it.
- **The Sleuth Kit:** It is a GUI-based suite that has a collection of different command-line tools used to find data in the disk and recovers files. It also allows the incorporation of additional modules for the analysis of data and the building of automated systems.

Challenges

The growth and development in technology have greatly affected the storage, transport, and processing of data in the digital landscape. Emerging technologies such as cloud and IoT have opened up a new front where the state of information security needs to be defended. Some of the corresponding challenges of these technologies onto the cyber forensic domain cloud could be listed as:

- **Data volume:** The colossal amount of data stored and processed by today's information technology platforms has created issues related to acquiring, storing, and processing data for forensic purposes. The multimedia-rich content today has further augmented the issue related to the explosion in the volume of data and its storage.
- **Data complexity:** Today, data is no longer confined to a single host, especially in the IoT network where the data is scattered across different physical or virtual nodes. The location itself may or may not be under the control of the jurisdiction of the group conducting the investigation. This issue is highlighted in cloud computing, where the task of data procurement is ladled with issues.
- **Development of standards:** The advances in technologies have compelled the research community to agree upon standards for file formats, schema, and ontologies. The investigation for crimes conducted using cutting-edge technology requires collaboratively processing information.
- **Privacy issues:** The forensic investigations related to online social networks and media sites pose many challenges related to privacy, as many people share personal aspects of their lives on such platforms.
- **Anti-forensics techniques:** Hackers today are increasingly using defensive measures such as encryption, obfuscation, and cloaking techniques, to hide their digital footprints.

Best Practices

To overcome the existing security challenges and recover evidence/data effectively, some digital forensics good practices need to be

followed whi`le conducting the investigation. Some of these are:

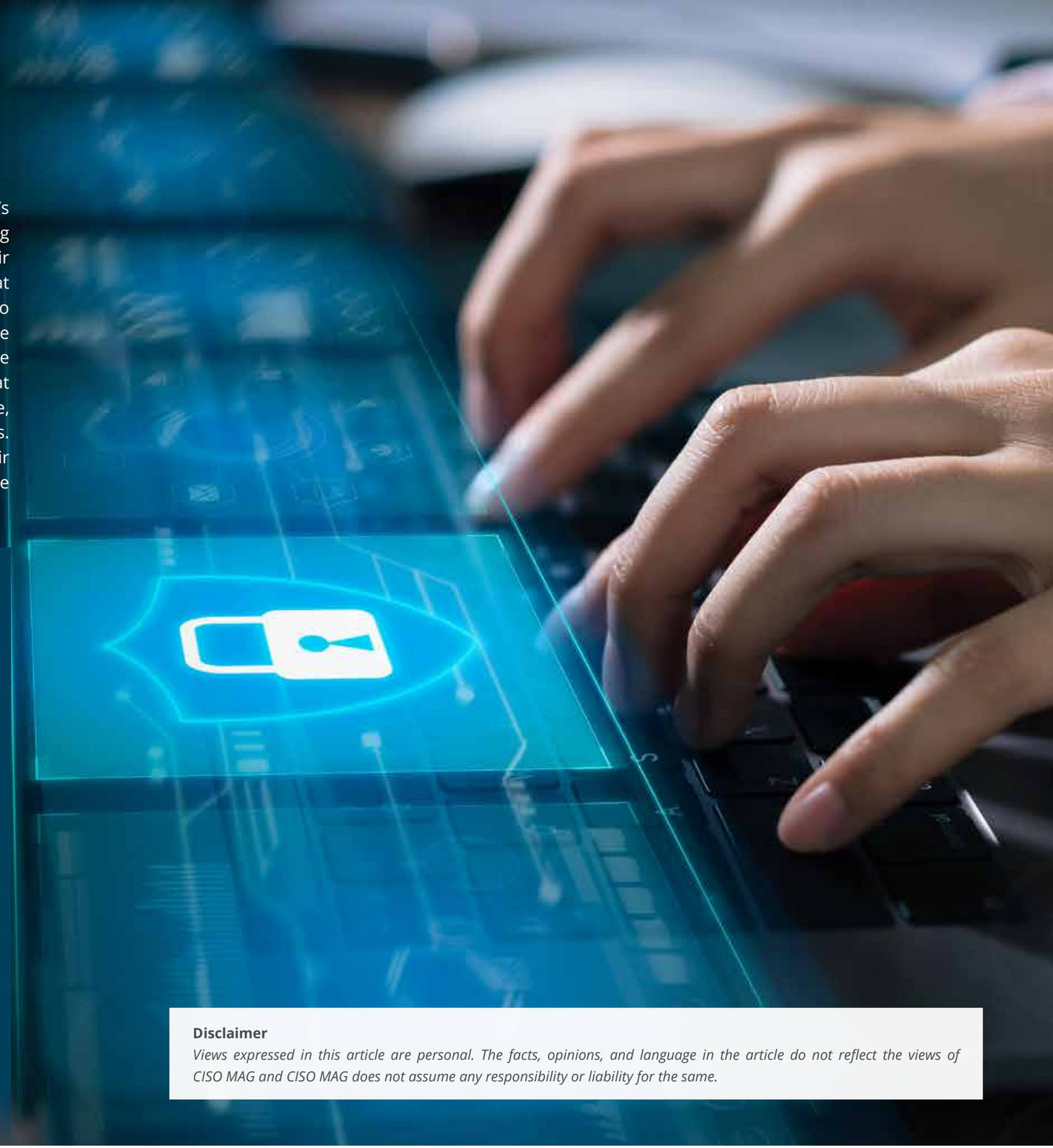
- Establish a proper plan and guideline in preparation for incident response and forensic practices.
- Secure the compromised/affected device along with its peripherals and removable media as part of incident response and forensic investigation.
- Prepare for device and data quarantined for forensics while simultaneously ensuring that business continuity is not affected.
- Have a thorough understanding of the device and data types involved in the investigation.
- Duplicate the data through memory drive cloning according to the norms and compliance.
- Use forensic approved storage drives to avoid cross-contamination of evidence.
- Follow the established guidelines for ethically identifying, collecting, analyzing, and reporting the data.
- Document every activity related to seizure, examination, storage, and transfer of digital evidence.
- Follow the guidelines for ethically persevering the data for legal requirements.
- The digital forensic investigator must act ethically and must conduct an accurate, unbiased, and independent analysis of the artifacts irrespective of their affiliation.

Conclusion

The state of cyber forensics in today's digital landscape is continuously evolving due to developing technologies and their implementation into cybercrime by threat actors. Malware is being developed to increase exploitation while covering the attackers' digital footprint to much possible extent. Hence, the forensic must look at these issues and develop its assets, scope, and policies to overcome these challenges. Organizations should develop and train their resources in the forensic domain and have this as a separate vertical.

About the Author

Anis Pankhania is a technology leader, with thorough understanding of adapting technology expertise to "business vision." He is an award-winning information security leader with 23 years of experience in leading the complete information security, infrastructure management, digitalization, application development and management, program/project management, IT network and data center operations, telecom circle/corporate/business operations, etc. Majority of his tenure has been spent with large telecom and IT companies in India (Bharti Airtel, Aircel, IBM and Vodafone). Pankhania established IT divisions from scratch, involving design of strategy & execution roadmap, objectives, operating procedures, multi-site facilities, end-user workspace for 30k+ end users.



Disclaimer

Views expressed in this article are personal. The facts, opinions, and language in the article do not reflect the views of CISO MAG and CISO MAG does not assume any responsibility or liability for the same.

Challenges and Applications of Digital Forensics

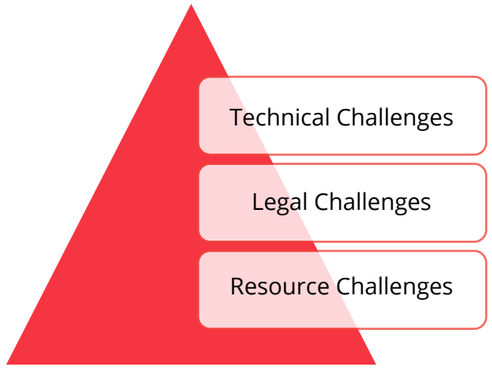
Priyanka S. Joshi
CISO - Risk and Control Specialist &
Technical Advisory
UBS

Crimes committed within the electronic or digital domains, particularly within cyberspace, have become general. They use technology as a footprint, commit offenses, and create new blueprints for law enforcement, attorneys and security professionals, and the legal departments. Digital Forensics has become an essential instrument in identifying and solving computer-based and assisted crime.

The digital age has undoubtedly revolutionized the life and work of many. On the flip side, the alarming rise in cybercrimes has become a major concern for cyber specialists as the continuous changes in the digital world attract more cybercrime. And experts use Digital Forensics to check this crime. Digital Forensics is the procedure of investigating computer crimes in the cyber world. The forensics process involves collecting, preserving, analyzing, and presenting the evidence from digital sources.

Digital forensics experts have devised scientifically proven methods for identifying, collecting, preserving, validating, analyzing, interpreting, and presenting digital evidence derived from digital sources to facilitate the reconstruction of events that led to a breach.

Let's discuss the major challenges of the digital world:



Technical Challenges: Encryption, data hiding in the storage space, covert channel are the major technical challenges today. Digital forensics experts use forensic tools for collecting shreds of evidence against criminals. And criminals themselves use such tools for hiding, altering, or removing the traces of their crime; this process is known as **anti-forensic techniques.** Another common challenge is **operating in the cloud, time to archive the data, skill gap, and steganography.**

Legal Challenges: There is an absence of guidelines and standards, and limitations of the Indian Evidence Act 1872. For instance, consider the case of dealing with the admissibility of an intercepted telephone call in a CDR (call data record). This was done without a certificate under Section 65B of the Indian Evidence Act, 1872. The court observed that the secondary electronic evidence without a certificate under Section 65B of the Indian Evidence Act, 1872 is not admissible and cannot be investigated by the court for any purpose whatsoever.

In most cases, the cyber police force lacks the necessary information that qualifies, and the ability to identify the possible source of evidence is unavailable. Often, the electronic evidence challenges the court due to its integrity, where the absence of proper guidelines and the non-availability of appropriate explanations of the details and acquisition gets dismissed.

Other common challenges are:

- Privacy issues
- Admissibility in the courts
- The preservation of electronic digital evidence
- Analyzing a running computer

Resource Challenges: Change in technology, volume and replication can be found in the resources area (Indian Evidence Act 1872). Due to rapid changes in the technology, operating system, and application software and hardware, reading digital evidence from an older version to support a newer version is a growing challenge. The confidentiality, integrity, and availability of e-documents are easily manipulated. In this, the WAN and the internet support a vast hand, which can share the data beyond physical boundaries, and creates the difficulty of understanding the origin of the data.

Application in Digital Forensics

The diversity of digital media and devices coupled with social media has led to the emergence of various branches of digital forensics such as Mobile Forensics, Network Forensics, Database Forensics, and Email Forensics.

The major applications of digital forensics are:

1. **Crime Detection -** Phishing, spoofing, and ransomware are the major examples. Also, various malware and malicious activities that happen over digital media.
2. **Crime Prevention -** Crimes that happen due to the lack of security or existing unknown vulnerabilities such as zero-day vulnerability, a major activity to prevent.
3. **Crime Analysis -** The investigation agents reconstruct the fragments of the data (searched by investigation) and draw a conclusion based on the evidence found.
4. **Preservation of Crime -** Protecting the crime scene and the digital evidence or setup from further manipulation and photographing and videographing the crime scene, for future reference. Also, this process involves stopping any ongoing command that may be linked to the crime.
5. **Identification -** This process involves identifying the digital media and devices that can serve as potential evidence.
6. **Extraction -** This process involves the imaging of the digital evidence, (to maintain the authenticity of the original evidence), for further analysis.
7. **Documentation -** This involves maintaining the chain of custody and documenting all the evidence collected from the crime scene.
8. **Interpretation -** The digital forensic expert prepares a report about the analysis conducted on the digital evidence, using various tools such as FTK (for imaging and mounting of evidence), Sleuth Kit and Autopsy (analyses disk images and recover files from them), and presenting it in the court of law. The conclusion is based on the evidence collected and reconstructing data fragments.

References

1. *Casey Eoghan. Handbook of Digital Forensics and Investigation. London. Elseveir Inc. 2010*
2. *Solomon G Michael, Rudolph K, Tittel Ed, Broom Neil, Barrett Daine. Computer Forensics Jumpstart. Canada. Wiley Publishing Inc. 2011.*

Importance in Today's Context

In the physical world, one tends to leave traces of oneself, such as fingerprints, clothes, hair strands, and DNA. Likewise, when we move into the digital world, we move and interact with people, places, and objects – and we leave digital traces, echoes of the activities we perform online. These virtual or digital traces include file fragments, activity logs, timestamps, and metadata.

These shreds of digital evidence can help establish the document's origins or pieces of the software for legal purposes. This helps determine the activities of the parties involved in the criminal activities – or even a resource for the criminals to plot or re-plot the information or to identify the data of their victims.

Robert Brown posted a quote on LinkedIn that says: "For the cybersecurity team whose role it is to protect the organization, or the investigators who are trying to establish how the business was breached, these bits of evidence are crucial. They will show how an incident happened, who was responsible, how to respond to it, and most importantly, how to stop it happening again in the future."

Techniques for Investigating Under Digital Forensics

- **Preserving the evidence:** This is done using common software tools that include Encase, Forensic Toolkit (FTK), SIFT, etc.
- **Web Activity Reconstruction:** Generally, the aim is to restore browsing history, temporary internet files, and accepted cookies.
- **File Signature Verification:** Compares header and footer information of suspicious files with known files.
- **Network Device Investigation:** Generally, involves network logs. The probe includes routers, switches, and firewalls to investigate suspicious DNS requests, connections to the unknown IPs or unexpected spikes in network activity.
- **Recovering Hidden Files:** Decryption, Cryptanalysis and drive-in image analysis to actively look for hidden data and files.

Best Practices in Digital Forensics

These are fundamental practices used for working on crime investigations.

- **Review your notes.** Always review notes for relevant information as this can ease the investigation.
- **Funnelling down information will help narrow leads to answers.** The first step of the investigation might have led the investigator to several IP addresses. Once an investigator finds a keyword that suspects a crime, for instance, a keyword such as "child pornography," the number of suspects owning the IP addresses can be narrowed down.
- **Eliminate or solidify evidence.** Always look at the information you gathered from a different perspective.
- **Watch your time.** The investigator needs to avoid distracting information. They need to consider the time wasted when they focus on the irrelevant.
- **Always analyze:** An investigator's report becomes useless without proper analysis. A computer forensic investigator is provided with high-technology software that helps in a thorough examination of the data retrieved and gathered.
- **Copy:** Evidence should always be copied or captured according to local procedures.
- **Seizing evidence has limitations.** Hence, it is crucial to investigate with an officer who can provide the necessary equipment and prevent tampering of evidence. A needle in a haystack can easily be found when you know which needle it is, and how it got lost in there.

Latest Trends and Developments and Legal Aspects and Legalities

The modern world is driven by social networks. The evolution in digital technologies has further evolved cybercrimes that significantly contributed to the development of new techniques, tools, and attacks that enable attackers to penetrate even in a well-controlled environment. With that said, security experts, academics, and law enforcement agencies use digital forensics to tackle the increasing number of cyber anomalies.

Market Snapshot

Source: Market Intelligence

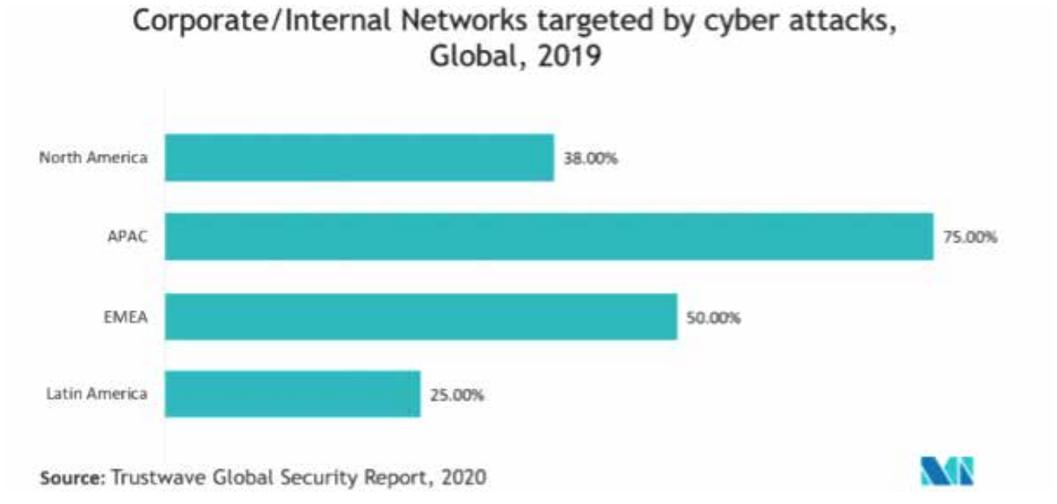
References
Digital Forensics Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021 - 2026) (mordorintelligence.com)

The digital forensics market was valued at $4,490 million in 2020 and it is expected to reach $8,210.5 million by 2026, registering a CAGR of 10.97% during the forecast period of 2021-26.

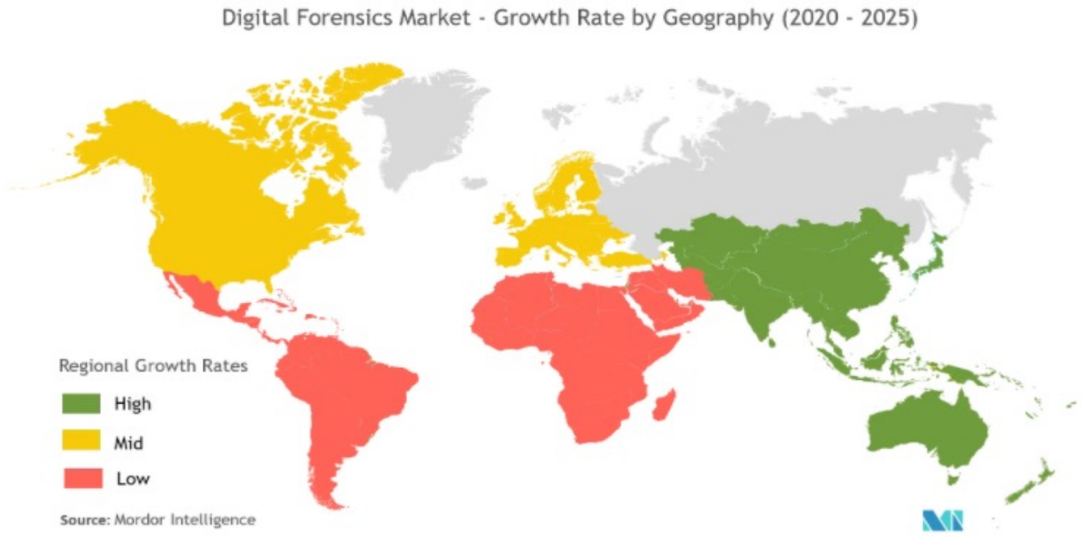
Most forensics is related to desktops, laptops, and associated media, including hard drives, removable media (USB external storage), and optical media. Form factors such as mobile and other handheld devices are becoming more detailed and popular.

- The adoption of digital forensics is growing due to advancements in the traditional crime lab infrastructure, increasing corporate penetration to the Internet Crime Complaint Centre (ICC) and Federal Bureau of Investigation (FBI). In 2019, 16,503 cases of online identity theft were reported to the IC3.
- COVID-19 will boost the digital forensics market as it helps tackle increased fraudulent activities. Europe is witnessing an increase in cybersecurity measures with the outbreak of COVID-19.
- Vendors in the market are also announcing solutions for controlling the COVID-19 pandemic. For instance, in 2019, MSAB (a global leader in forensic technology for mobile device investigations), announced that its technology could be used to assist first responders, law enforcement officials, public health officials, and others involved in controlling the current coronavirus pandemic. The technology uses mobile phone data to identify where individuals have been, whom they have been in contact with, and their activity timeline, along with other key information that might be needed.
- However, factors, such as lack of specialized skills, usage of proprietary operating systems, and high level of encryption in new mobile applications, may hinder the growth of the market.

Key Market Trends



Digital Forensic Market



Conclusion

Digital forensics, sometimes known as digital forensic science, is fundamental to investigations performed in reality. Modern digital societies are subject to cybercrime activities. There should updates for forensics tools that should be engineered to support the heterogenous investigations, privacy data, and scalability — to preserve important data. The use of different tools and techniques poses new problems due to their differences in data storage, accessibility, and investigative trade-offs.

About the Author

Priyanka Joshi is a Risk and Control Specialist/Technical Advisory at UBS. As an infosec professional, she believes knowledge and experience are pathfinders to success. Joshi also believes in maintaining the company's legal and ethical integrity. Before joining UBS, Joshi was a Compliance Manager at a small firm for a health care company based in the U.S., where she was responsible for the HIPAA security enforcement on the business software and people working for it.

References:
- *Casey Eoghan. Handbook of Digital Forensics and Investigation. London. Elsevier Inc. 2010*
- *Solomon G Michael, Rudolph K, Tittel Ed, Broom Neil, Barrett Daine. Computer Forensics Jumpstart. Canada. Wiley Publishing Inc. 2011.*
- *Digital Forensics Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021 - 2026) (mordorintelligence.com)*

THE DARK SIDE OF THE ATTACK ON COLONIAL PIPELINE

Augustin Kurian
Assistant Editor
CISO MAG

At daybreak on May 7, an employee of Colonial Pipeline found a ransom note on a control-room computer. The signs were clear, a ransomware attack had just targeted one of the largest oil pipeline systems of the U.S. The engineers immediately locked the systems to contain the spread of the attack to its 260 delivery nodes across 13 states. It took them over an hour to successfully complete the shutdown procedure, eventually preventing its operational technology (OT) systems from getting infected. But, by then, the damage was done.

The scale of the attack was unprecedented, to say the least. The attack had compromised the billing system, eventually leading to a halt in pipeline operations. The company had to shut down the pipeline as a precaution due to concerns that the attackers may have obtained information allowing them to carry out further attacks on vulnerable parts of the pipeline. Apparently, the attackers had also stolen nearly 100 gigabytes of data and threatened to release it on the internet if the ransom was not paid.

In the days that followed this incident, fuel shortages began to occur at filling stations, caused by panic buying, with states like Alabama, Georgia, Florida, North and South Carolina reporting gas shortages. In some cases, 71% of filling stations ran out of fuel. American Airlines changed flight schedules temporarily after the shortage hit Charlotte Douglas International Airport. Consequentially, several flights had fuel stops or plane changes added to their schedules for four days. Airports directly serviced by Colonial Pipeline had to look for alternatives.

Eventually, the government had to intervene, and President Joe Biden declared a state of emergency removing limits on the transport of fuels by road. Several states also waived taxes on diesel and gasoline. The situation was so dire in certain parts of the country due to panic buying that the U.S. Consumer Product Safety Commission had to issue an advisory asking people to “not fill plastic bags with gasoline” (an obvious fire hazard).

Colonial paid the DarkSide too

Within hours of the attack, Colonial's team was not sure about the extent, time, and cost of getting back up and running. This led the CEO, Joseph Blount, to make a difficult decision – paying up. In an interview with the *Wall Street Journal*, Blount acknowledged that he authorized the ransom payment of 75 Bitcoins, which approximately accounts for $4.4 million.

"I know that's a highly controversial decision. I didn't make it lightly. I will admit that I wasn't comfortable seeing money go out the door to people like this. But it was the right thing to do for the country," Blount said.

Whether paying the ransom was the right thing to do or not, as Blount said, it was indeed highly controversial.

Colonial engaged cybersecurity firms and third-party security experts to investigate the incident and informed law enforcement and the Department of Energy about the attack. In the early stages of the investigation, several industry experts opined that ransomware group DarkSide was likely behind the cyberattack. DarkSide ransomware group is known for encrypting systems with ransomware and extorting victims to pay the ransom.

In the ensuing days, DarkSide released a statement stating that its "goal is to make money, and not creating problems for society."

This was probably the second biggest ransomware attack only after Wannacry that had such a massive scale of real-world consequences.

The Risks of Paying Ransom

Charles Brook
Threat Intelligence Specialist
Tessian

Paying the ransom is sometimes an option but it is high risk. You should always work with a security consultant to advise on the whole process and handle the negotiations - ideally have one on retainer - and you should inform law enforcement.

For most ransomware, it is in the attacker's interest to provide decryption keys upon receiving payment. This means they maintain a good reputation, which can promote further payouts by other victims and lead to increased financial gain for the attacker.

However, some ransomwares may go for a "double dip" which means that once you pay the initial ransom demand, they will continue to withhold the decryption key and ask for more money. Sometimes, you may never receive a decryption key and attackers will just continue to ratchet up the price to see how much they can get from you.

Other ransomware only exists to disrupt or destroy. NotPetya is considered to have been a wiper disguised as ransomware. Even when payment was made the attackers did not provide decryption keys.

The biggest implication of the cyber attack

"The largest implication would be its impact on national security. Unfortunately, our aging infrastructure is extremely vulnerable to attacks like this, making it an easy and lucrative target. Just because we only hear about these types of incidents on our critical infrastructure once in a while, doesn't mean that more advanced attackers from nation-states are unable to get in. It's highly probable that they're already present, which should be even more concerning. Organizations in charge of critical infrastructure should be required to adhere to specific cybersecurity standards, or even be required to obtain certain compliance certifications, which get audited yearly. We should be past the point of recommending best practices to critical infrastructure given the increasing number of sophisticated actors and the impact these attacks can have," said Tim Bandos, CISO and VP of Managed Security Services at Digital Guardian.

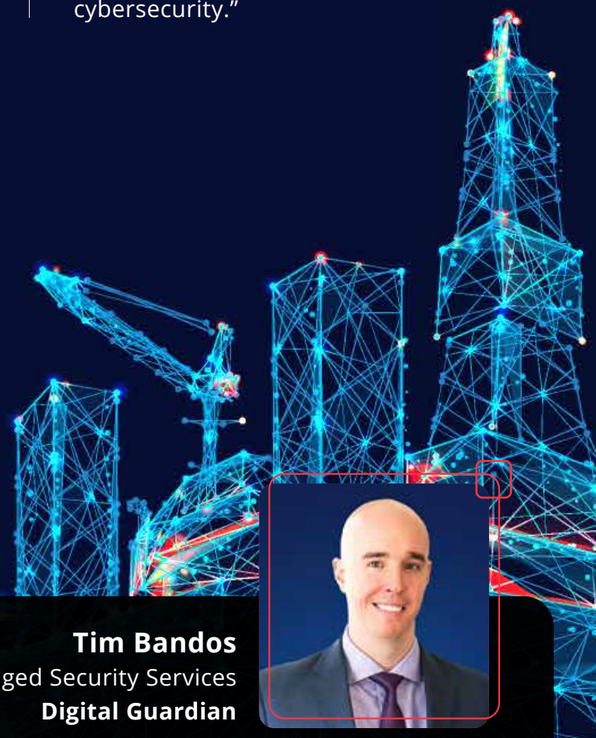
Several incidents also highlighted how ransomware gangs were indiscriminately targeting critical infrastructure. Many a times, these infrastructures supported important economic activities which may not be limited to the business itself. Ron Brash, Director of Cyber Security Insights, Verve Industrial, pointed out, "Many organizations – even society – are generally unable to consider consequences that are beyond their own boundaries or at scale, and this incident demonstrates that such an important piece of infrastructure seemingly had large failings that an opportunistic actor took advantage of. Whether DarkSide is apolitical or not, their claim is moot because Colonial was the third critical infrastructure organization they compromised. It's all about the money/revenue generation from ransom, and that needs to be changed."

Ron Brash
Director of Cyber Security Insights
Verve Industrial

> Incidents such as this one have a drastic effect on the economics of society, futures trading, supply and demand, and civilian panic (well-founded or not). And because the global supply chain is starting to wear thin (like too little butter on too much toast), events like this demonstrate the fragility of the system today, but also demonstrate a massive and overdue investment opportunity.

He continued, "Incidents such as this one have a drastic effect on the economics of society, futures trading, supply and demand, and civilian panic (well-founded or not). And because the global supply chain is starting to wear thin (like too little butter on too much toast), events like this demonstrate the fragility of the system today, but also demonstrate a massive and overdue investment opportunity. In the past, such large investment projects have also brought about prosperity as they did during the 1960s/1970s and this should be looked at similarly."

Another implication will likely be the increased focus of the U.S. government on private sector cybersecurity. According to John Livingston, CEO, Verve Industrial, "Regulation is almost always the result of a major event. NERC CIP was in large part due to the Northeast blackout of 2003. To date, TSA has been the regulator of pipeline security and its focus has primarily been on physical attacks. The biggest impact of Colonial will almost certainly be a shift to a more robust compliance regime for the whole energy value chain…beyond just electricity. We have already seen the announcement of the President's new executive order. My belief is this is just the beginning of what will be a significant shift in private sector requirements for those industries considered 'critical infrastructure'. If this turns out as we expect, this will have a massive impact on the investment and focus on private sector cybersecurity."



Tim Bandos
CISO and VP of Managed Security Services
Digital Guardian

> The largest implication would be its impact on national security. Unfortunately, our aging infrastructure is extremely vulnerable to attacks like this, making it an easy and lucrative target. Just because we only hear about these types of incidents on our critical infrastructure once in a while, doesn't mean that more advanced attackers from nation-states are unable to get in. It's highly probable that they're already present, which should be even more concerning.

How did the government respond?

In the wake of the attack, the U.S. House Committee on Homeland Security passed seven bipartisan security bills to bolster defense capabilities, enhance pipeline security, and defend supply-chain attacks targeting U.S. organizations and critical infrastructure.

The Bills include:

- The Pipeline Security Act (H.R. 3243), introduced by Congressman Emanuel Cleaver, will enhance the ability of TSA — the principal Federal entity responsible for pipeline security — to guard pipeline systems against cyberattacks, terrorist attacks, and other threats.
- The State and Local Cybersecurity Improvement Act (H.R. 3138), introduced by Congresswoman Yvette D. Clarke, seeks to authorize a new $500 million grant program to provide State and local, Tribal, and Territorial governments with dedicated funding to secure their networks from ransomware and other cyberattacks.
- The Cybersecurity Vulnerability Remediation Act (H.R. 2980), introduced by Congresswoman Sheila Jackson Lee, will authorize CISA to assist critical infrastructure owners and operators with mitigation strategies against the most critical, known vulnerabilities.
- The CISA Cyber Exercise Act (H.R. 3223) establishes a National Cyber Exercise program within CISA to promote more regular testing and systemic assessments of preparedness and resilience to cyberattacks against critical infrastructure. The bill was introduced by Congresswoman Elissa Slotkin.
- The DHS Blue Campaign Enhancement Act (H.R. 2795) strengthens the DHS Blue Campaign and enhances the availability of human trafficking prevention training opportunities and the development of such training and materials. The bill was introduced by Congressman Peter Meijer.
- The DHS Medical Countermeasures Act (H.R. 3263), introduced by Congresswoman Mariannette Miller-Meeks, establishes a medical countermeasures program to support DHS mission continuity and facilitate the readiness and resilience in the event of a chemical, biological, radiological, nuclear, or explosives attack, naturally occurring disease outbreak, or pandemic.
- The Domains Critical to Homeland Security Act (H.R. 3264), introduced by Ranking Member John Katko, authorizes DHS to conduct research and development into supply chain risks for critical domains of the U.S. economy and transmit the results to Congress.

The attack had also prompted the Biden administration for an Executive Order (EO) specifically aimed at improving the current state of the nation's cybersecurity. The EO stated:

- The IT service providers are now mandatorily required to notify the government about cybersecurity breaches that could impact U.S. federal and public networks. The EO states that any contractual barriers that might stop providers from threat intel sharing can now be bypassed as it is in the best interest of the nation.
- A standardized playbook and set of definitions that will help federal agencies to give a prompt response to future cyber incidents.
- Recommendation to the federal government to upgrade their operations to secure cloud services and other cyber infrastructure. Apart from this, a mandatory deployment of multifactor authentication and encryption for all data accessed, stored, and communicated, is necessary.
- Software service providers rendering services to the Federal Government agencies are now required to improve the security of the software sold to the government, which also includes its developers sharing certain security data publicly. The EO also recommends employing a zero-trust model and security in all software modules in a ground-up manner.
- A new "Cybersecurity Safety Review Board" comprising public- and private-sector officials will soon be formed which can give expert advice and analyze the situation making recommendations post a cyberattack or breach incident.
- The EO creates cybersecurity event log requirements for federal departments and agencies. Robust and consistent logging practices solve latency issues of investigation and remediation measures.
- An intra-governmental robust information sharing will be established to provide Government-wide Endpoint Detection and Response (EDR) deployment.

Cybersecurity and legal teams have historically been operating in silos but this needs to change. AJ Shankar, CEO of Everlaw, spoke about how to go about eliminating these silos — and the pitfalls that will continue if the departments remain separate.

He said, "President Biden's recent cybersecurity executive order has been a forcing function for security teams embracing new workflows and partnering more seamlessly with all teams within an organization. Corporate legal departments have an exciting opportunity to seize the moment and partner with their CIO to discuss their unique technology needs. In-house legal teams often handle some of their company's most sensitive and confidential data, and law firms face an even more daunting security challenge, having to manage the highly confidential and privileged data of all their clients. In the last year alone, 29% of law firms reported a security breach, and we saw this play out most recently when hackers compromised the servers of a high-profile law firm and leaked gigabytes of highly sensitive data. We're going to keep seeing this play out until this gap between security and legal teams is bridged. We see a great opportunity for both in-house legal teams and law firms to invest in domain-specific tools that offer much higher levels of security and compliance than what they might be using today."

AJ Shankar
CEO
Everlaw

President Biden's recent cybersecurity executive order has been a forcing function for security teams embracing new workflows and partnering more seamlessly with all teams within an organization. Corporate legal departments have an exciting opportunity to seize the moment and partner with their CIO to discuss their unique technology needs. In-house legal teams often handle some of their company's most sensitive and confidential data, and law firms face an even more daunting security challenge, having to manage the highly confidential and privileged data of all their clients.

Tony Pelli
Security and Resilience Practice Director
BSI

> As far back as February 2020 (following another pipeline-related cybersecurity incident), the Department of Homeland Security indicated that owners of critical infrastructure should take specific measures to reduce or lessen the risk of ransomware attacks. The agency highlighted a lack of cybersecurity knowledge and the inordinate amount of attention paid to physical emergency and incident scenarios in preparation and planning.

How much of the responsibilities fall on Colonial Pipeline?

In short, quite a lot, even after negating the entire fact that the company went ahead and paid the ransom to the attackers, which is "illegal" according to an advisory by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC).

"The hack of the Colonial Pipeline – which provides about 2.5 million of the 8 million barrels of oil used in the U.S. each day – shows the importance of preparation and proper risk assessment in avoiding and mitigating supply chain disruptions and how cybersecurity incidents can have serious real-world impacts. As far back as February 2020 (following another pipeline-related cybersecurity incident), the Department of Homeland Security indicated that owners of critical infrastructure should take specific measures to reduce or lessen the risk of ransomware attacks. The agency highlighted a lack of cybersecurity knowledge and the inordinate amount of attention paid to physical emergency and incident scenarios in preparation and planning. This incident should serve as a reminder to companies in all industries, but especially those in more "physical" industries such as supply chain, logistics, and shipping, that they are not immune from cybersecurity incidents and should incorporate those threats into their risk assessments," said Tony Pelli, Security and Resilience Practice Director at BSI.

Concurring with Pelli, Bandos said, "Typically, ransomware attacks are successful because organizations neglect to implement even the most basic security measures and are not being properly prepared. The types of questions that need to be posed to Colonial Pipeline are, 'How prepared were they for an attack like this?' and 'What types of security gaps were taken advantage of here that facilitated the success of this attack?' If we learn that Colonial Pipeline had major issues with their security program, then there should be a level of accountability placed on them for being at least partially responsible. Ransomware attackers typically seek out targets with 'low hanging fruit' vulnerabilities. Identifying and removing these types of vulnerabilities is imperative in addition to implementing appropriate security measures."

John Livingston
CEO
Verve Industrial

> Your absolute priority is to know your plan if you are hacked. What is the response plan if you see devices being ransomed? What can you stop? How do you reduce the spread? Secondly, practice the basics of cybersecurity. You want to make it harder to attack you than it is to attack your neighbor.

What should be learnt from the attack?

Organizations should realize that nobody is immune to these types of cyberattacks. Bandos added, "Simply hoping that it won't happen to you puts your organization at risk of becoming the next victim on a news headline with significant business impact to match. All organizations in the critical infrastructure sector need to be prepared and have a formal incident response process in place as well to ensure decisions are being made quickly to recover as fast as possible. This attack merely highlighted that services like heat, light, and transportation can be threatened and stopped in an instant by a small team of hackers halfway around the world."

Cyber basics go a long way, and organizations need to invest in correcting decades of security rot and build the foundations of successful backbones to their business for tomorrow. If you "do security right," generally, you can get a lot of wins tomorrow, and lowered TCO while remaining efficient. "Critical infrastructure or industry is not off limits to ransomware. It's opportunistic, so be ready, be prepared, and be tested to recover at scale. It should be a part of every organization's practiced end-to-end training curriculum!" said Ron Brash.

To conclude, "Your absolute first priority is to know your plan if you are hacked," said John Livingston. According to him, it must begin from understanding, the response plan and your methods to stop, and reduce the spread of an attack. He continued, "Secondly, practice the basics of cyber security. You want to make it harder to attack you than it is to attack your neighbor. So, "lock the doors," and "put up outside lights". The cyber equivalent is to patch your critical devices, ensure network protection devices like firewalls and switches are properly configured to segment critical assets, ensure no dormant or inappropriate accounts or users on the system."

With inputs from Rudra Srinivas and Mihir Bhagwe

About the Author

Augustin Kurian the Assistant Editor of CISO MAG. He writes interviews and features.

Jérémy Thomas
Co-founder and CEO
GitGuardian

"Public GitHub is often a blind spot in the security team's perimeter"

GitHub and the community surrounding it have changed the way the world uses and builds open source components and software. At present, there are more than 50 million developers using GitHub; 60 million repositories are created in a single year, with over two billion contributions. With such a vast resource of data publicly available, there is also an abundance of sensitive data that is unknowingly or accidentally pushed to the platform, namely secrets like API keys, credentials, and other digital authentication strings. These secrets can be used by attackers to gain access to infrastructure, systems, and PII.

It will still be a mammoth task to quantify the problem that arises due to the public GitHub. To evaluate that, **Augustin Kurian, Assistant Editor** of ***CISO MAG***, has interviewed **Jérémy Thomas, Co-founder** and **CEO** of **GitGuardian**. Thomas is an engineer and an entrepreneur. A graduate from Ecole Centrale in Paris, he first worked in Finance and then began his entrepreneurial journey by first founding Quantiops, a consulting company specializing in the analysis of large amounts of data, then GitGuardian in 2017.

In this interview, Thomas talks about the exposure of secrets within public repositories on GitHub and how this threat is evolving year on year. He also talks about the responsibilities of CISOs to ensure their developers do not accidentally leak secrets, Intellectual Property, or PII, and the best practices that need to be established.

UNDER THE SPOTLIGHT

Recently, an unknown actor compromised the official PHP Git repository and pushed backdoored code under the guise of a minor edit. And these are a common affair. With organizations oftentimes taking most of their codes from Git repositories, don't you think this is a major cybersecurity issue?

Indeed, leveraging open source dependencies comes with both risks and opportunities for organizations. On one side, organizations don't have to reinvent the wheel and can reduce their time-to-market by easily importing external open source software in their codebase, in the form of dependencies. If carefully chosen (not all open source codes are equal), these dependencies are battle-tested at unprecedented scales, scales that only the open source can allow. There are 50 million developers on GitHub. These developers collaborate publicly, write code, test code, solve bugs, and deploy code in various environments. The more a code snippet is deployed in as many environments as possible, the more it is tested, the more eyeballs are on it, the safer it is. However, it happens that certain dependencies contain vulnerabilities (just like every software does). In such cases, the huge scale of the open source can become a downside, because the vulnerable code is instantly deployed in so many environments. Hence the need for Software Composition Analysis tools to have visibility about components imported in the codebase, their version and vulnerability status, so that they can be patched quickly when a vulnerability is discovered.

> On one side, organizations don't have to reinvent the wheel and can reduce their time-to-market by easily importing external open source software in their codebase, in the form of dependencies. If carefully chosen (not all open source codes are equal), these dependencies are battle-tested at unprecedented scales, scales that only the open source can allow.

PHP is thought to underpin almost 80% of websites. This includes all WordPress sites, which are built on PHP. With malicious actors pushing backdoors for remote code execution (RCE) like the earlier incident mentioned, do you think these can result in a much larger-scale attack surface? How does GitGuardian come into this picture?

Backdoors are a particularly major cybersecurity issue especially if they remain undetected for extended periods. This is only compounded when these backdoors are added to technology which, as you say, underpins many websites and web applications. Another example backdoor recently discovered was for CodeCov's continuous integration (CI) tool. This backdoor was undetected for months and allowed the attackers to steal sensitive information from users' CI environments.

Many think of security as building a wall around your assets and infrastructure, the core idea being to keep intruders out. While this wall is important, there are multiple ways an attacker can penetrate past this wall, a backdoor as we just discussed is one example. It may be a backdoor in your application, in the underpinning technology of your application such as the PHP example or as part of your application environment as was the case with the CodeCov example. This means we need a shift in how we approach security that considers what happens when the walls are breached. Solutions can help ensure sensitive information is not exposed to attackers even in the event of an intrusion. For example, GitGuardian Internal Monitoring solution scans for sensitive data within internal Version Control Systems and alerts users in real-time if any are discovered. This means that even if an attacker gains access to these internal systems via a backdoor or any other method we can prevent them from using secrets to move laterally into different systems.

According to a GitGuardian study, there has been a 20% year-on-year increase in the number of secrets – such as application programming interface (API) keys, private keys, certificates, usernames, and passwords – discovered on a public repository. What measures must CISOs take to ensure that the data of their organization must not be among these secrets?

CISOs are starting to realize that even if their company has limited official activities on public GitHub, their developers most certainly use the platform regularly. The difficulty for security teams is that public GitHub is often a blind spot in their security perimeter. It is difficult for organizations to identify developers' public activity on personal repositories without a proper solution. Our report indicates that many corporate credentials are found on developers' personal repositories, where CISOs have no visibility and no authority to enforce any kind of preventive security measures. On top of this, most organizations underestimate the number of secrets that are exposed within their internal repositories. And this, even if they deployed secrets management solutions. As code is a very leaky asset, widely accessible within the organization, it is critical that CISOs secure their Software Development Lifecycle by implementing efficient secrets detection.

Sixty million repositories were created last year, representing a 35% increase over the previous year. On the flipside, cybercriminals are now actively scanning repositories looking for secrets that would enable them to compromise applications. What tips should developers keep in mind while pushing code to GitHub?

The best practices for developers include:

1. They should scan their code to verify there are no secrets in their Git history. Git is an iceberg-like environment and the current version, the tip of the iceberg, is not the only part of the code that should not contain secrets. It is important to remember that this is not just the current version of the project

that is made public, but all changes and iterations too.

2. If any secret is found by the secrets detection solution, they must rotate their credentials and optionally remove the secrets from Git history. Here is a cheatsheet they can follow.
3. If they want to shift left their security, they can even implement secret detection as a pre-commit hook. The earlier a vulnerability is uncovered, the less costly it is. This way the developer can catch the secret locally and prevent it from reaching the server.

Can you give us an example of a recent breach leveraging credentials?

I will illustrate this with a white hat attack on the Indian Government. The white hat group named Sakura Samurai did a huge breach that spans across multiple different state-owned entities. In total, a lot of information was found, including 35 separate sets of exposed credential pairs, three instances of a very sensitive file disclosure, five exposed private RSA keys, 13,000 PII records, dozens of sensitive police reports, and forensic reports. They also discovered remote code execution on a financial server and then in the end, they hijacked an application running on that financial server. After establishing a perimeter and potential vulnerabilities, they searched for secrets to make their initial access, and they found 10 Git directories with hardcoded credentials. They were also able to find 23 exposed env files, which are environment variable files and regularly used to set up the environment of an application. These make them a very high-value target for attackers. From there they were able to move laterally and breach more deeply, but this is a long story.

You have mentioned the shift left testing approach. Can you give us an example? How does secret detection serve this purpose?

Shifting left is about making security more developer-centric, and giving developers security feedback where they are, when they are coding. A good example of shift left testing put into practice is the implementation of automated vulnerability detection at each incremental change made by developers. This is exactly what you do when implementing an automated secrets detection system. The advantage of this early detection is dual: on the one hand, you limit the cost of development as you can fix early and on the other hand, you keep your developer in the loop. They are in context and can respond to alerts as they code. Real-time is far better than days later at deployment or months later from a penetration test report. And this is critical in terms of vulnerability exposure and cost of remediation.

About the Interviewer

Augustin Kurian the Assistant Editor of CISO MAG. He writes interviews and features.

INSIGHT

How to Know When it's Time to Break Up with Your Tech Provider

Tim Bandos
Chief Information Security Officer
Digital Guardian

Even if your organization doesn't want to address it, there comes a time when every company needs to take a step back, take stock of their technology stack, and ask themselves if it's time for a change.

It's not your fault – let's say your organization has grown, not just in size but in business maturity, since you first implemented your current vendor. It may be the case that the provider hasn't had the capacity or means to scale along with you.

While not always easy to know when the time is right, there are three tell-tale signs that you've outgrown your provider.

Lack of innovation

If your provider isn't staying on top of the latest technology – solutions that can add value to your business and empower employees to learn new skills and execute their work at a high level – it may be time to look elsewhere. Maybe your company has grown too comfortable with legacy technology. Its drawbacks may seem like slight annoyances to you. Still, it could indicate a larger problem or a missed opportunity to cut costs or add customer value with new alternative technology. Your vendor should be proactive in keeping you apprised of the latest technology and solutions, especially if they can help your company become more economical and productive.

Every organization wants to stay focused on maintaining its competitive edge, especially in a market as volatile as the one today. If your vendor isn't doing their part – investigating in interoperability, so your organization can get a greater return from the sum of your tech investments – it should set off a red flag.

Does your vendor have a CISO? Do they use safe APIs? Are they using DevOps? Have they moved to the cloud for added speed and flexibility? If you answered "no" to any of these questions, you might want to ask them – why not?

Maybe your provider was recently bought and absorbed by another corporation. Whenever a company is acquired and a business changes hands, there's a lot in flux. With change, it's not unusual to have some questions about the direction your vendor may be going. With an acquisition, corporate reshuffles are commonplace. Could this impact leadership, engineering, and budget at a vendor you use? Are you willing to trust a company and its vision despite these changes?

In some instances, when a tech company is acquired, innovation is stifled, and the acquiring company does little more than maintain the product. Acquisitions can also result in cutbacks on support resources and failure to invest in new features that help ensure the security of their software.

That's not to mention that old, depreciated technology can put your employee and customer data at risk. As more and more companies can attest these days, experiencing a data breach can pose a risk to your company's brand and have a serious effect on carrying out day-to-day business. Your organization is part of a supply chain; it's essential to ensure that every vendor you partner with is following best practices.

It's not you, it's me (your needs have changed)

As I hinted earlier, maybe your organization has grown since you first implemented your current technology vendor, and they haven't been able to keep up. Perhaps your business has grown so fast that your needs have changed from what they once were.

If your vendor isn't keeping up by periodically performing audits to ensure that policies and

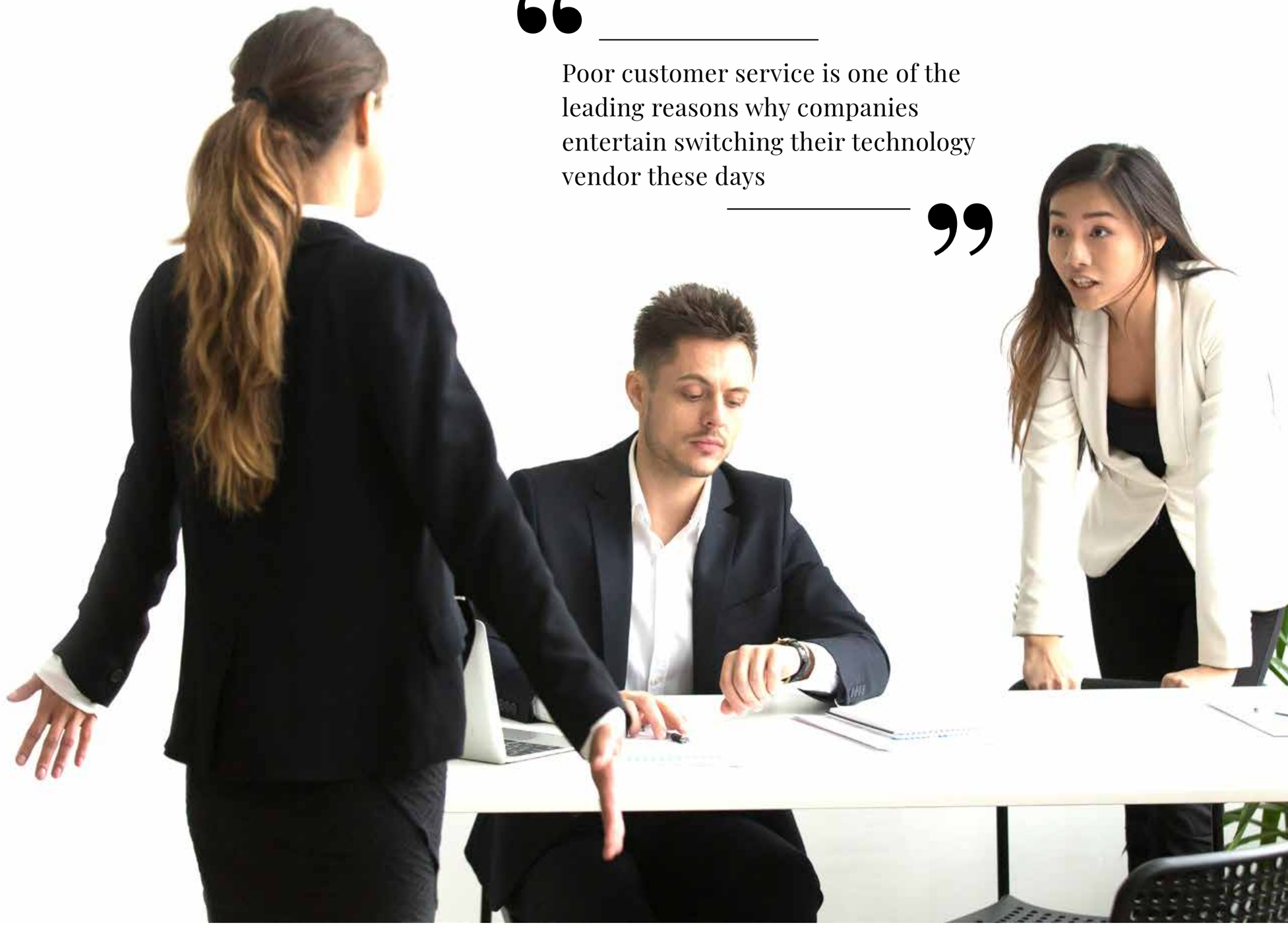
procedures you have in place are effective in meeting those needs, you may have blind spots in your coverage. Your vendors' IT services should be tailored to meet you. The old marketing slogan, "set it and forget it," rarely applies to your technology stack. Staying with a vendor that isn't constantly evolving alongside your business could be hurting your company's bottom line.

Perhaps your organization has elected to move away from the rigidness of the waterfall software development method and go the agile route to deliver products rapidly and to better respond to changes in your environment. If so, you know that creating a truly agile team requires a big cultural shift and reduced organizational resistance. If your vendor isn't agile or does something to hold you back from fulfilling that cultural change, you may need one better suited to complement your needs.

Depending on your space, shifting regulatory compliance requirements can often dictate a company's needs. Satisfying governance, risk management, and compliance (GRC) requirements demand a higher degree of attention. It's one thing to tick checkboxes associated with regulations like HIPAA, GLBA, and SOX. All of them, in addition to state, federal, and global legislative requirements, require organizations to have the appropriate technical safeguards in place.

To keep up with evolving regulations, especially those slated to take effect soon, organizations need a higher level of

> Poor customer service is one of the leading reasons why companies entertain switching their technology vendor these days



engagement, planning, and collaboration from their vendors. Ensuring there's visibility across all your critical assets to identify data, the organizational policies they're governed by, and whether it complies, is essential to navigating the risk landscape, too. Your provider should be aware of these changing regulations and offer advice and guidance on satisfying them if they're not already.

The vendors you use are integral to your company's success – they help drive growth, revenue, and goals. If yours aren't, it's time to reevaluate those relationships.

The relationship is strained

There's a chance your vendor relationship has reached a stalemate or has run its course. Like any good partner, yours should be keeping your best interests top of mind.

Vendor lock-in, a situation when a customer becomes forcibly dependent on a vendor or product, can be a real problem for organizations. Sometimes it can get to a point where the costs and difficulties associated with switching seem almost insurmountable. If your provider is strong-arming your organization and taking advantage of the high cost of switching from their product to raise licensing continually, subscription, or support prices, it needs addressing. Becoming too dependent on a vendor and fearing the repercussions around switching is a textbook sign that you're at an impasse.

Having to deal with a seemingly endless line of support tickets or a messy support workflow, where it's challenging to get status updates, could be a sign it's time for a change, too.

Poor customer service is one of the leading reasons why companies entertain switching their technology vendor these days. Remember: their technology is supposed to enable your business, not hold it back. If your vendor is serious about their relationship with you, their customer service should speak for itself.

We've already discussed why vendors should adopt new technologies to help them better respond to customer needs. Suppose your vendor isn't doing something to remedy negative support experiences, resolve churn, or address the lag between customer support requests – in that case, you know firsthand how quickly the negatives outweigh the positives.

Transparency and visibility are also vital. Lack of communication around known product issues, bugs, product management road maps, and scheduled maintenance dates can leave you in the dark. It often translates to downtime and lost revenue.

Vendors who proactively reach out to customers to make these issues known and communicate other issues generally succeed at reducing churn. For some companies, nurturing that company-customer relationship via a customer success program is a strategic imperative. After all, how can a business run smoothly if you, their customer, aren't happy?

Customer success programs often deliver value to both parties and can often be the reason customers renew their contracts with vendors. If your vendor doesn't run a customer success program and your questions to support continue to fall on deaf ears, it can often feel like screaming into the void. If you're not happy with your current relationship and your vendor isn't working to remediate your issues, why are you continuing to stay in the relationship?

I've recently worked with several customers who have come to us after experiencing these three tell-tale signs with their current vendors. Some were finally looking to migrate their solution to the cloud and have a more innovative experience. Others felt like their relationship wasn't going anywhere, and their current vendor did not support the capabilities they needed today. It's critical to re-evaluate your security stack each year to ensure you're receiving a return on your investment and keeping up with the ever-evolving threat landscape.

In one case, we had a client who was no longer happy with their vendor, and they were unable to run their data protection solution themselves due to a lack of resources and time. We were able to fill this gap for them and provide a complete 24/7 managed service offering that fulfilled their needs.

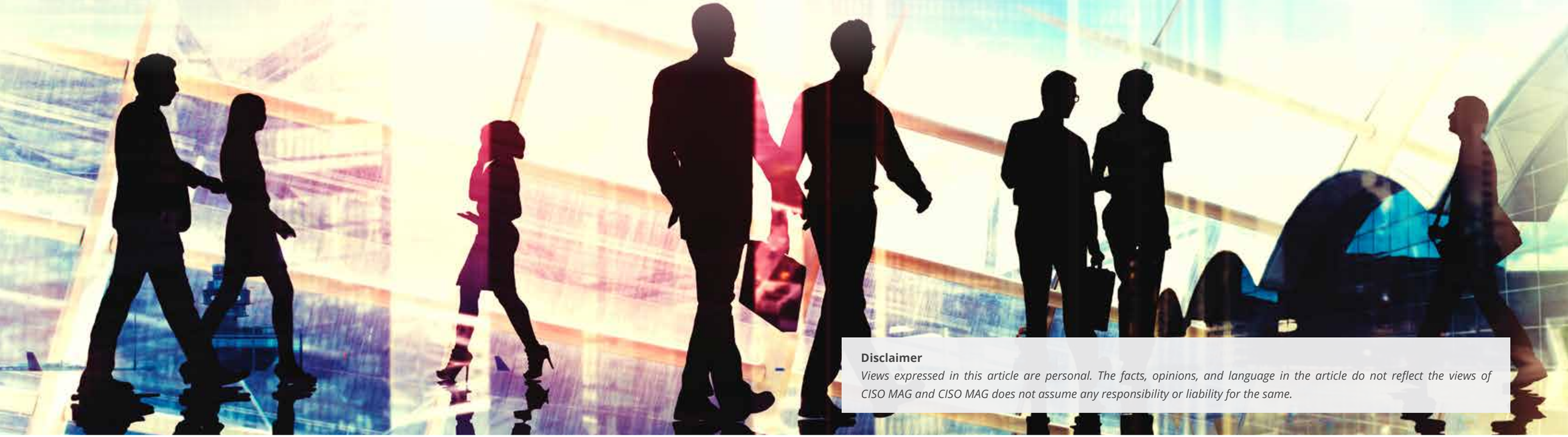
Organizations that incorporate these security stack evaluations as a part of their overall maturity program tend to have a greater likelihood of success and ultimately reduce their level of risk to the company.

It's also essential to ensure that, during the evaluation period, your team can continue to support the stack you've implemented. As time goes on and responsibilities shift, it's possible that running these tools in-house is no longer viable. Consolidation is key. If you have existing solutions that offer additional services, it will make managing your stack a lot easier. Fewer vendors provide fewer relationships to manage, and you'll have a higher purchasing power.

Changing, or even just beginning to think about changing IT vendors, takes time. If yours isn't meeting your needs and some of these signs sound familiar, it may be time to look for an alternative. While identifying the right security stack that works for you and your organization may require a significant amount of planning, the more you simplify, with quality tools and solutions over quantity, the better.

About the Author

Tim Bandos was recently announced as the Chief Information Security Officer (CISO) for Digital Guardian. He has over 15 years of experience to the position including his five years as VP of cybersecurity at Digital Guardian. Prior to joining Digital Guardian, Bandos was Director of Cybersecurity for Dupont where he was responsible for overseeing internal controls, incident response, and threat intelligence.



Bringing Forensics Education Up to Speed

By EC-Council Cyber Research & Computer Hacking Forensic Investigator Teams

Novel criminal activities in the digital landscape always accompany the trends and development in technology, and consequentially, digital security lags. The same could be true for digital forensics (DF), especially in its education curriculum, which has encountered significant obstacles over the last decade, and now stands at the crossroads of development.

Cyber/digital forensics, without a doubt, has become an integral part of the cybersecurity domain. Due to increasing cyberattacks against individual users, corporate organizations, and even states, have taken the security of their digital assets more seriously. The role of digital forensics is to examine the attack and to detect the attacker's digital footprint to identify the vulnerabilities that were missed by the multiple layers of security deployed.

Today, the world is largely dependent on global data connectivity for its functioning, decimated across various networks, systems, mobile and smart devices. This complex environment has given rise to multiple opportunities for threat actors to conduct e-crimes. The adoption and widescale implementation of emerging technologies such as cloud computing, Internet of Things (IoT), and Blockchain, have further augmented the existing security issues, and digital forensic is no exception. "The state of cyber forensics in today's digital landscape is continuously evolving due to developing technologies and their implementation into cybercrime by threat actors. Malware and other attacks are being developed to increase exploitation while covering the attacker's digital footprint to the much possible extent. Hence, forensics must look at these issues and develop its assets, scope, and policies to overcome these challenges," says Anis Pankhania, CISO – Cloud Infrastructure Services, Capgemini India.

Anis Pankhania
CISO – Cloud Infrastructure Services,
Capgemini India

"The state of cyber forensics in today's digital landscape is continuously evolving due to developing technologies and their implementation into cybercrime by threat actors. Malware and other attacks are being developed to increase exploitation while covering the attacker's digital footprint to the much possible extent. Hence, forensics must look at these issues and develop its assets, scope, and policies to overcome these challenges.

It is entirely logical for organizations and businesses to think first about their technical and market performance. They readily tend to incorporate the latest developments in information technology into their business operations. But these developments may increase the risk if information security isn't adequately implemented. In some cases, security measures deployed for the protection of consumer privacy end up hindering the forensic process during its data acquisition stage, making it more difficult for the digital forensic analyst to ascertain the cause more accurately. Cloud computing technology is an apt example for such issues, where the artifacts required for forensics is in the custody of the cloud service provider.

In the *CISO MAG* "Implementing Digital Forensics in Emerging Technologies" survey included in this issue, more than 60% of the respondents believe that organization factors (63.84%) and the legal factors (76.01%) do have a significant influence over cloud forensics readiness of any organization. Apart from technological elements, the volume of data that these emerging technologies create and store has also become a major hurdle. The amount of

data is directly proportional to the amount of digital evidence and artifacts that need to be analyzed in the given period.

Impact on Digital Forensics Education

Digital forensics cannot be mastered by unifying skills and experience acquired by various practitioners. Aspirants could learn and thoroughly understand the concepts and technology involved in digital forensics through course training and certifications. The underlying perspective for any DF education revolves around teaching the concepts of collecting, preserving, examining, analyzing, and presenting digital evidence in a form that would be admissible in a court of law.

Since digital forensics is about the aftermath of any incident, the curriculum for many DF education programs and certifications revolves around the existing technologies and widely known genres of cases.

New technology could be implemented without fully understanding the security implications of each of its actions. That leads to an unprecedented series of threats and cyberattacks due to misconfigurations. The digital forensics education domain is thus at a crossroads. The challenges posed by these emerging technologies have a significant impact, and an analyst is expected to solve these challenges by default. So, there is dependence on the personal experience and technology understanding of the analyst. Hence, it is imperative for digital forensic experts, universities, certification bodies, and the digital forensics community to come together and understand where we are currently, where we need to go, and how we can get there.

Where are we currently?

Today, most organizations mandate certification or a degree as a prerequisite, with experience for the digital forensics investigator/analyst role. The aim here is to hire forensics-ready investigators, which also complies with the goal of the forensics readiness policies.

Certification and accreditation are essential to attach validity to the evidence while presenting it in a court of law. Without a relevant degree or certificate, it has become difficult for an investigator to claim to be an expert in computer forensics to validate the evidence.

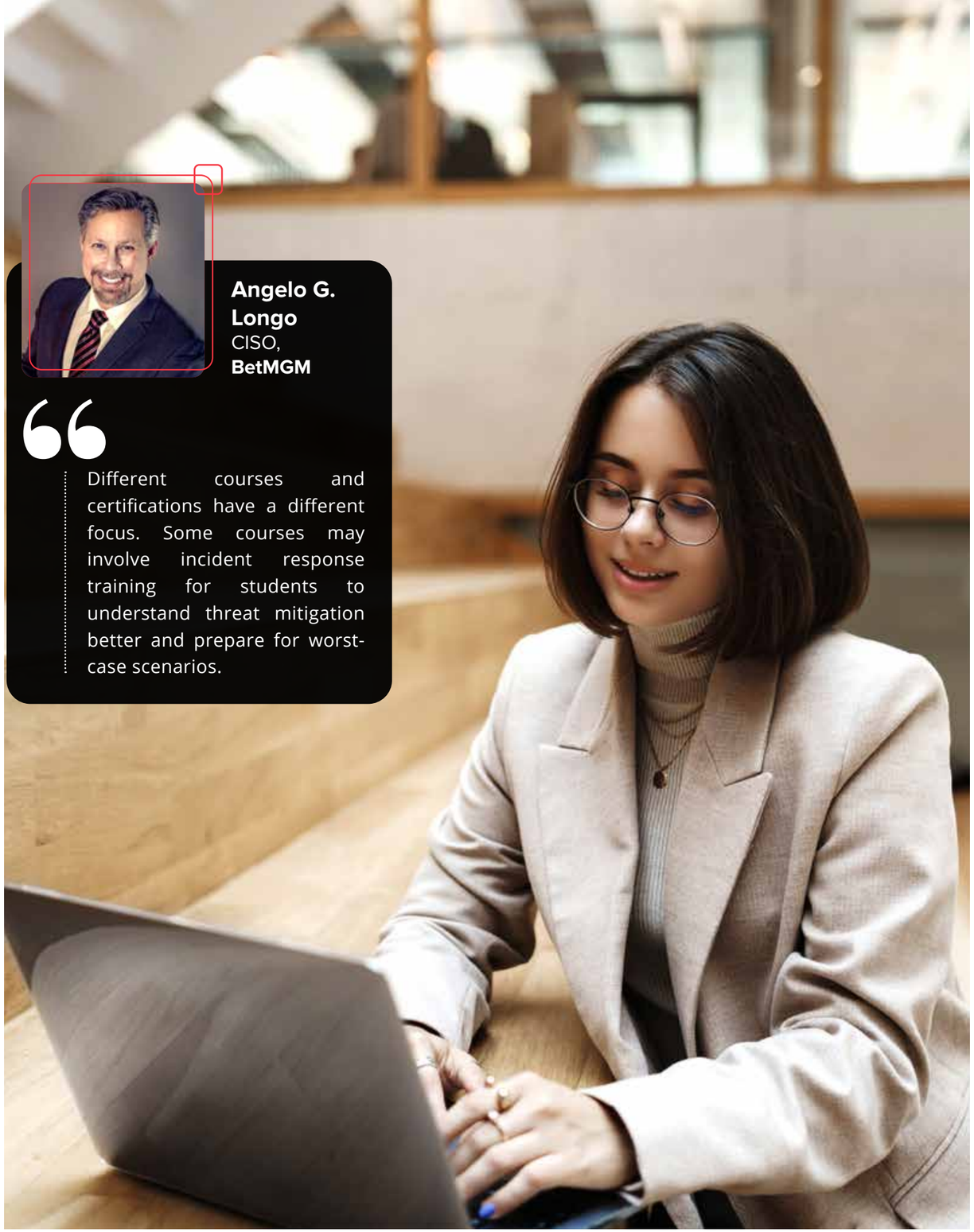
Today, digital forensics has become a required approach for organizations to develop their information security infrastructure further. There are multiple courses for digital forensics education in both physical and online learning modes. These cater to the digital forensic education needs at undergraduate and master's levels of information technology curricula. These certification programs provide holistic and

specialized courses that include training to handle different software and toolkits and practice data sets to gain practical knowledge.

“Different courses and certifications have a different focus. Some courses may involve incident response training for students to understand threat mitigation better and prepare for worst-case scenarios,” says Angelo G. Longo, CISO for BetMGM. “Whereas some focus is needed on establishing a security policy framework and its management. Apart from this, supplementary teaching can elaborate on investigation techniques and methods to prepare the students for performing forensic investigation under diverse environments.”

Longo recently published a whitepaper entitled “Computer Forensic Education Guidance for 2021,” and we quote from his paper.

The general focus of any digital forensics training program revolves around technical content and the operational procedures involved in the investigation process, such as data recovery, artifact identification, extraction, and report writing. The concepts involved in technical training tend to discuss some of the most critical problems concerning the forensic investigation processes today. These concepts could be categorized under several sections or modules: hard disks and file systems, data acquisition and duplication, anti-forensics techniques, operating system forensics, network forensics, web forensics, database forensics, malware forensics, email forensics, and mobile forensics.



Angelo G. Longo
CISO,
BetMGM

> Different courses and certifications have a different focus. Some courses may involve incident response training for students to understand threat mitigation better and prepare for worst-case scenarios.

Where do we need to go?

Emerging technologies and trends have impacted digital forensics in a significant way. The consensus in the community is that the current state of forensic readiness and education is in chaos and flux. Considering emerging technologies such as IoT, Blockchain, and cloud, the fundamental concepts and abstract thinking techniques are not adequately developed and introduced into curricula and practice.

The limitation of current training programs is that they are not balanced with specializations of new technologies, and those that do may or may not correspond to industry needs. Besides, the lack of coherence between the curriculum and quality of training leads to program differences between certifications.

The emerging technologies that need to be incorporated and further researched into digital forensics education include cloud forensics, data recovery, IT forensics, Dark-web forensics, and IoT forensics.

Cloud forensics currently poses multiple challenges for investigation in the cloud environment. As the nature of the cloud is closely associated with multitenancy, multi-jurisdiction, data duplication, and a high degree of virtualization, this adds to the multi-layer complexity of forensics in a cloud environment.

The data recovery program, especially the recovery of encrypted data, impacts the forensics capabilities of any organization

towards information security. Forensics analysts need to understand decryption using open source or existing keys regarding ransomware, as ransomware continuously grows in scale and performance ability.

IoT forensics involves more than what current cyber forensics covers. It is a vast network of multiple devices linked together across various networks, transmitting data across multiple layers of connectivity. IoT involves multiple devices, networks, applications, protocols, processing architectures, and information dissemination layers. And this expands the scope of digital forensics in terms of artifact identification and extraction.

Dark-web forensics could be categorized into browser forensics (TOR) and Bitcoin forensics. Whereas the former is similar to that of regular browser forensics, i.e., to obtain the information present within the browser. The latter aims to draw information related to the cryptocurrency, as most malicious transactions in the darknet take place in the form of digital currency.

How do we get there?

To accommodate emerging technologies into a security architecture, more research must be done into how these technologies interact with existing platforms. Then one needs to design and implement digital forensics techniques and protocols around it.

Apart from developing tools and techniques, the focus should be on creating a global consensus with regards to establishing widely acceptable policies and frameworks. Many of the technologies are affected by the regional government's compliances and laws. Hence, there must be a common policy framework that could be agreed upon by all the governments and stakeholders across the globe.

A trend that is bound to incorporate itself into the digital forensic education curriculum is gamification and interactive learning. These methods of learning provide hands-on experience and improve learning efficiency for examining case studies, competitions, lifelong learning skills, research & development.

The crux of any research into trends in the market and technology lies in knowing what the current challenges are and then working upon them to develop a solution. With regards to this, *CISO MAG* conducted a survey this year on "Implementing Digital Forensic in Emerging Technologies."

The study and the corresponding report examine the current and future challenges in digital forensics and how the latest developments in the existing forensic technologies affect the community. The report analyzes the impact and the current understanding of the forensic readiness of organizations and how it is subjected to digital forensics education.

SURVEY

MARKET TRENDS REPORT

IMPLEMENTING DIGITAL FORENSICS IN EMERGING TECHNOLOGIES

To better understand the challenges and state of readiness in implementing Digital Forensics (DF) in emerging technologies, *CISO MAG*, in collaboration with EC-Council's CHFI (Computer Hacking and Forensic Investigation), launched a Technology Trends Survey in April 2021. The report offers an in-depth analysis of how important it is to incorporate the effects of digital forensics on emerging technologies into the curriculum of digital forensic education.

This survey is oriented towards skills, training, and industry opportunities, specifically for digital forensics.

This exclusive report, based on the survey, showcases the viewpoints of industry experts and their perspectives from across the table.

SURVEY

Aim

The survey aims to better understand the forensic readiness and challenges of implementing digital forensics in emerging technologies. The widespread adoption of technologies such as the Internet of Things (IoT), cloud computing, mobile and web applications has changed the way data is being processed and stored. From the perspective of cybersecurity education in digital forensics, this survey attempts to gauge the upcoming challenges that will arise upon deeper integration of digital forensics with these technologies.

Methodology

This report is based on the results of an online survey conducted by *CISO MAG* for its readers. The survey was conducted using a system that is integrated with EC-Council's enterprise systems.

Questions for the survey were vetted by CISOs, industry experts, and advocates in the field of digital forensics. On closure, *CISO MAG* editors further discussed the findings of the survey results with industry experts, which helped in deriving an expert commentary while analyzing and interpreting them.

Key Findings

94.83% of the respondents believe that cloud computing technology and its corresponding cloud forensics will have a greater impact on digital forensics education in the future.

60.51% of the respondents feel that gaining evidence files of around 50 GB for digital forensics study and research, will be extensively or quite helpful, as there is a general lack of high-volume data in forensics for study and practice.

52.40% of the respondents believe that smartphones connected to, or as an IoT device will be the most challenging task while performing IoT forensics.

39.11% of the respondents believe that performing forensics of a network is the most challenging task when conducting TOR forensics.

86.72% of the respondents believe that analyzing and decrypting will be the widely used methods for dealing with the anti-forensics technique of encryption.

SURVEY

Survey Respondent Profile

(In alphabetical order)

- Analyst
- AppSec Manager
- Associate Manager
- Auditor
- Business Analyst
- Business Applications Support Officer
- CEO/Founder
- Chairman
- CIO
- CISO
- Co-Founder & Director
- Compliance Leader
- Consultant
- CTO
- Cyber Investigations Head
- Cyber Security Engineer
- Cyber Security Researcher
- Data Analyst
- Detective
- Digital Forensics Analyst
- Director Director of Operations
- Director of R&D
- Graduates
- GRC Manager
- Information Security Analyst
- Information Security Engineer
- Information Security Head
- Information Security Manager
- Information Security Officer
- Information Security Operation manager
- Information Technology Manager
- Infrastructure Specialists
- Integration Engineer
- IS Compliance Officer
- IT Administrator
- IT Analyst
- IT Auditor/Risk manager
- IT Director/IT Development Manager
- IT Engineer
- IT Head
- IT Security Analyst
- Lead Investigator
- Network Admin
- Network Engineer
- Network Threat Analyst
- Pentester
- Professor
- Project Manager
- Security Administrator
- Security analyst
- SOC Analyst
- Software Engineer
- Student
- Tech Lead
- Technical Manager
- Threat Hunter
- VP
- VP of Cloud and Container Security
- Web Developer

72 Countries

The **271 validated respondents** represent a cross-section of organizations and institutes across 72 countries, as listed below.

1. Afghanistan
2. Australia
3. Bahamas
4. Bangladesh
5. Botswana
6. Brazil
7. Bulgaria
8. Cambodia
9. Cameroon
10. Canada
11. Chile
12. China
13. Colombia
14. Cote d'Ivoire
15. Croatia
16. Cyprus
17. Czech Republic
18. Democratic Republic of the Congo
19. Deutschland
20. Egypt
21. Estonia
22. Ethiopia
23. France
24. Germany
25. Ghana
26. Greece
27. Hong Kong
28. Hungary
29. India
30. Indonesia
31. Iraq
32. Ireland
33. Israel
34. Italy
35. Kenya
36. Lebanon
37. Malawi
38. Mauritius
39. Mexico
40. Morocco
41. Myanmar
42. Namibia
43. Netherlands
44. Nicaragua
45. Nigeria
46. Norway
47. Oman
48. Pakistan
49. Peru
50. Philippines
51. Poland
52. Portugal
53. Saudi Arabia
54. Sierra Leone
55. Singapore
56. Slovakia
57. South Africa
58. Spain
59. Sri Lanka
60. Tanzania
61. Thailand
62. Togo
63. Trinidad and Tobago
64. Tunisia
65. Uganda
66. Ukraine
67. United Arab Emirates
68. United Kingdom
69. United States of America
70. Vietnam
71. Zambia
72. Zimbabwe

Jenai Marinkovic
CISO/CTO
Tiro Security, USA

One of the most significant risks to the forensics field are breaches where threat actors leverage and exploit artificially intelligent systems.

Forensics professionals must become skilled in digitally recreating a successful attack against a thinking system and attacks that leverage AI-based digital weapons.

We must also consider the legal implications, especially around how we implement the principles of forensically sound processes (meaning, errors, transparency and trustworthiness, reproducibility, and experience) when dealing with AI systems that use black-box models at their core.

Rakesh Sharma
VP – Cloud & Container Security
Standard Chartered Bank
Singapore

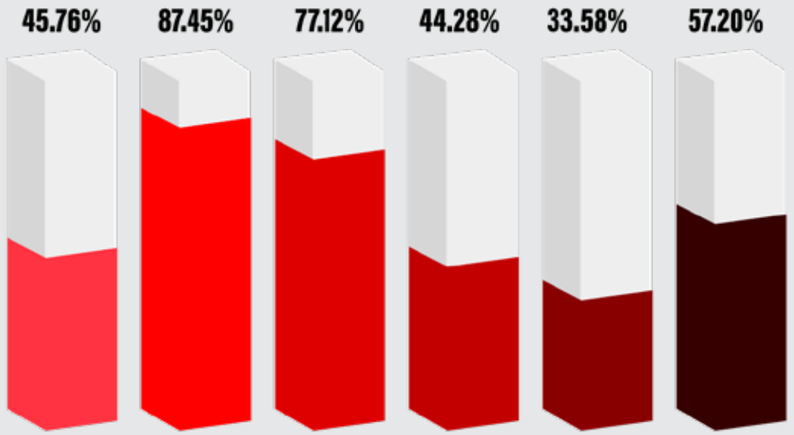
Advanced data recovery techniques and tools are required when performing data acquisitions from emerging technology platforms including ephemeral infrastructure. Emerging technologies will continue to shape digital forensics but the most powerful tool we have at our disposal is our brain. Critical thinking will continue to evolve and will be highly required in threat analysis and breach investigations.

Makoma Toona
Senior Consultant –
IT Forensics
Control Risks,
South Africa

Digital Forensics has become an integral part of most forensic investigations. The process involves the use of multiple tools, techniques, and qualified experts to uncover evidence residing in electronic devices and networks. It is imperative to use experienced and qualified personnel to ensure that proper handling and examination of evidence is applied. In recent times, there has been an urge for organizations to consider digital transformation following the repercussions caused by the global pandemic. This has presented a need for Digital Forensics investigators to consider using advances in artificial intelligence (AI), robotics, and the Internet of Things (IoT) to handle challenges such as large data volumes during investigations. These advances can be embedded in Digital Forensics tools and the investigation workflow; to ensure efficient results during current and future investigations. Digital forensic experts have to keep abreast with the latest trends and upskill themselves in order to stay relevant and to understand the incorporation of 4th industrial revolution into the expert work.

SURVEY

What qualities and skills are important for a digital forensics (DF) analyst?



(More than one option was selected)

45.76%	Case awareness	44.28%	Patience and perseverance
87.45%	Analytical skills	33.58%	Understanding your role in the entire process
77.12%	Technical skills	57.20%	Ethical and compliance knowledge

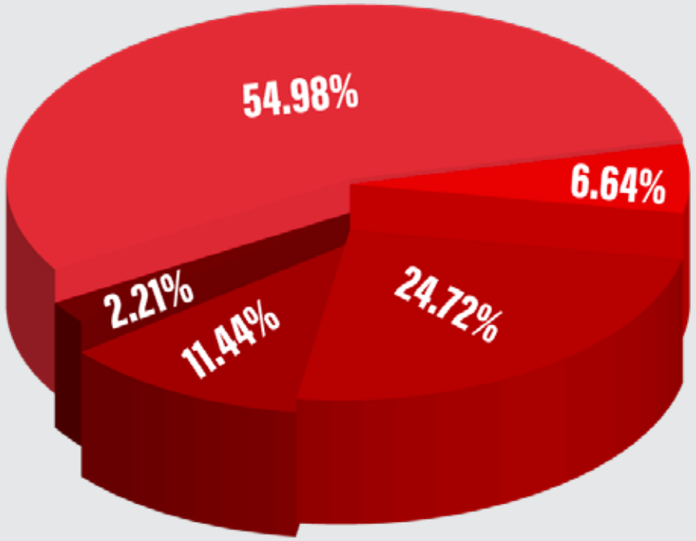
Base: 271 respondents.

The present state of digital forensics education is continuously changing due to the impact of emerging technologies on information security. Hence, along with the tools and technologies, those pursuing digital forensics must possess a certain set of skills. As to which skills are of prime importance, the survey results indicate that analytical skills (87.45%), technical skills (77.12%), and ethical skills and compliance knowledge (57.20%) were most favored. Those who have the right combination of these three skills will excel in their careers as DF specialists. Though other skills such as case awareness (45.76%), patience and perseverance (44.28%), and understanding your role in the entire process (33.58%) were deemed necessary but not as prominent as the former.

SURVEY

Why are digital forensics certifications important?

Digital forensics programs and certifications have become too specialized to adapt to continuously evolving technological advancements. Since many cybersecurity professionals transit from IT, obtaining a digital forensics certification has become important to advance one's career in this domain. Nearly 55% of the respondents feel that the main reason these certifications could be considered important is that they validate and improve the forensic knowledge of an individual.



54.98%	They improve and validate the forensic knowledge of an individual	11.44%	They signify the forensic readiness of the workforce
6.64%	They are considered a selection criterion for hiring	2.21%	Other
24.72%	They create confidence in an individual's ability to meet forensic challenges		

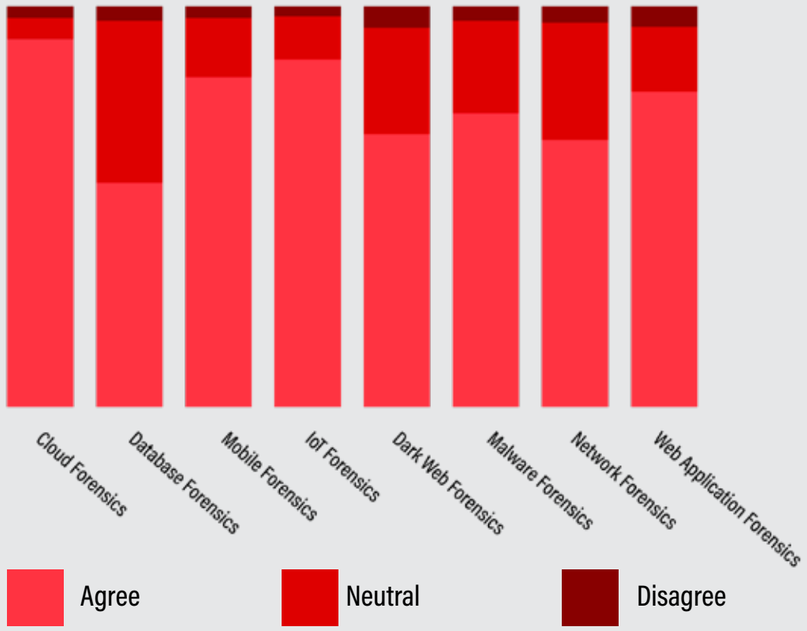
Base: 271 respondents.

54.98%
They improve and validate the forensic knowledge of an individual

24.72%
They create confidence in an individual's ability to meet forensic challenges

SURVEY

Which emerging technologies do you agree/disagree with, will have a greater impact on digital forensics education in the future?



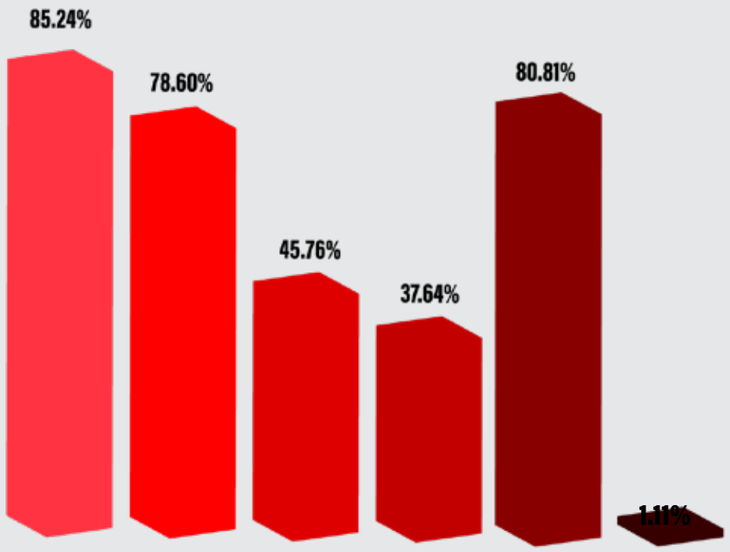
- **Cloud Forensics:** 94.83% Agree; 4.80% Neutral; 0.37% Disagree
- **Database Forensics:** 67.90% Agree; 31.36% Neutral; 0.74% Disagree
- **Mobile Forensics:** 84.87% Agree; 14.76% Neutral; 0.37% Disagree
- **Internet of Things (IoT) Forensics:** 87.45% Agree; 11.81% Neutral; 0.74% Disagree
- **Dark Web Forensics:** 74.91% Agree; 23.24% Neutral; 1.85% Disagree
- **Malware Forensics:** 78.60% Agree; 20.66% Neutral; 0.74% Disagree
- **Network Forensics:** 73.06% Agree; 25.46% Neutral; 1.48% Disagree
- **Web Application Forensics:** 80.07% Agree; 18.08% Neutral; 1.85% Disagree

(More than one option was selected) Base: 271 respondents.

Emerging technologies such as cloud computing, mobile and IoT have changed our current understanding of data storage, processing, and transport across the digital landscape. This has led to the increase in risk posed to information security. The same is also true for the applications, browsers, networks, and malware that are evolving and developing continuously. Hence, all this is increasing their respective impacts on digital forensics. Among the various technologies that may greatly impact the future of digital forensics education, the top three selected are Cloud forensics (94.83%), IoT forensics (87.45%), and Mobile forensics (84.87%).

SURVEY

Which areas do you believe are challenging, or require further research to understand the forensics of fileless malware?



(More than one option was selected)

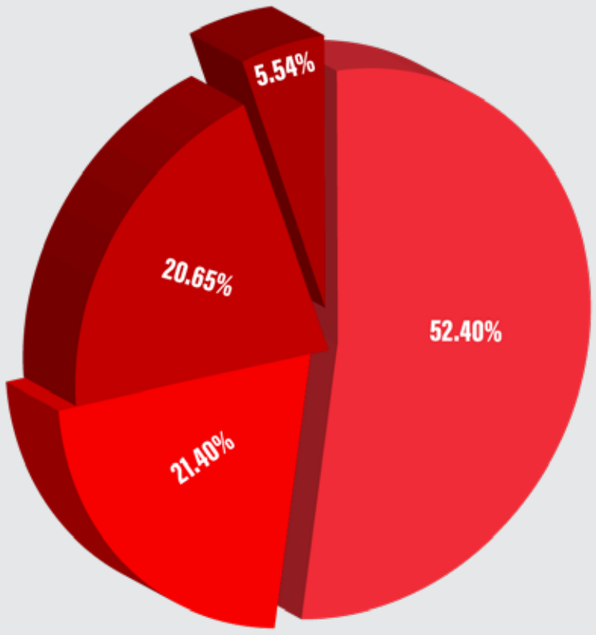
85.24%	Fileless malware infection chain	37.64%	Understanding the malware attack via documents
78.60%	Understanding the malware attack via memory exploits	80.81%	Analysis of fileless malware
45.76%	Understanding the malware attack via websites	1.11%	Other

Base: 271 respondents.

The evolving threat landscape contains one of the most potent cybersecurity risks known as fileless malware; it does not use the file system to carry out its attack, which helps it evade many security barriers such as signature-based detection systems. Thus, forensic measures are among the limited solutions to detect these catastrophic attacks, but it still has its challenges. Most of the respondents feel that understanding the malware infection chain (85.24%), its analysis (80.81%), and understanding malware attacks via memory exploits (78.60%) are the prime challenges faced during its forensic analysis.

SURVEY

Which IoT devices, do you believe, face the most challenges while performing digital forensics?



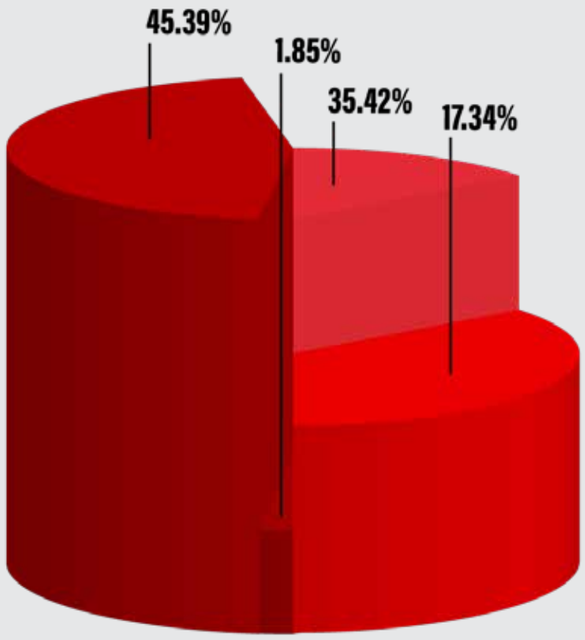
52.40%	Smart phones	20.65%	Smart watches
21.40%	Smart speakers	5.54%	Other

Base: 271 respondents.

IoT forensics tends to include more than what conventional cyber forensics covers and is not just a mere part of digital forensics as it includes multiple layers across the internet and the interconnected device for data transmission and storage. Thus, conducting forensics for IoT devices is considered a challenge, and many of the respondents feel that smartphones are more challenging (52.40%) to conduct forensics than other IoT devices such as smart speakers (21.40%), smartwatches (20.66%), and others (5.54%).

SURVEY

As a cloud user, which "cloud service" model do you believe would present the most challenges during cloud forensics?



35.42%	IaaS (Infrastructure as a Service)	45.39%	SaaS (Software as a Service)
17.34%	PaaS (Platform as a Service)	1.85%	Other

Base: 271 respondents.

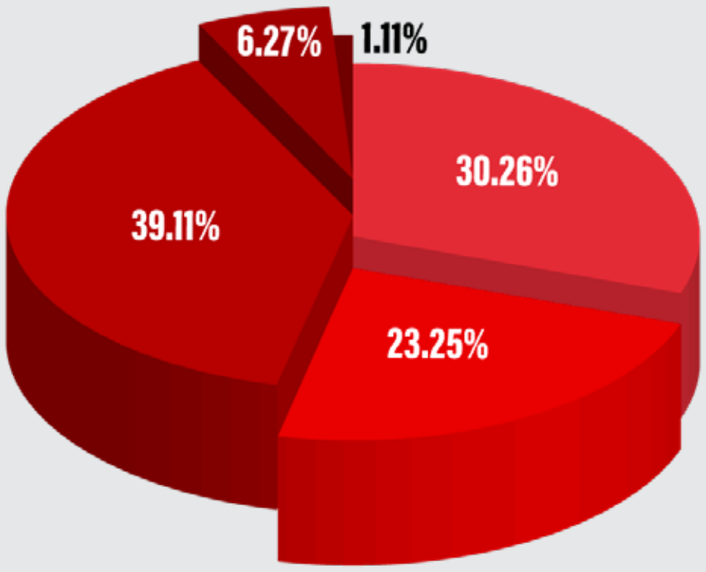
Cloud forensics is a cross-discipline application of digital forensics for the data stored in the cloud environment. As cloud servers are expensive, most organizations rely on cloud service providers to provide different types of cloud services such as IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service), etc. But, for forensic investigators, obtaining the data hosted with third-party systems that also host data from other clients is quite troublesome. Even with the presence of service level agreements (SLA), many of the respondents feel that working out digital forensics with SaaS (45.39%) is more challenging when compared to IaaS (35.42%) and PaaS (17.34%).

35.42%
IaaS (Infrastructure as a Service)

45.39%
SaaS (Software as a Service)

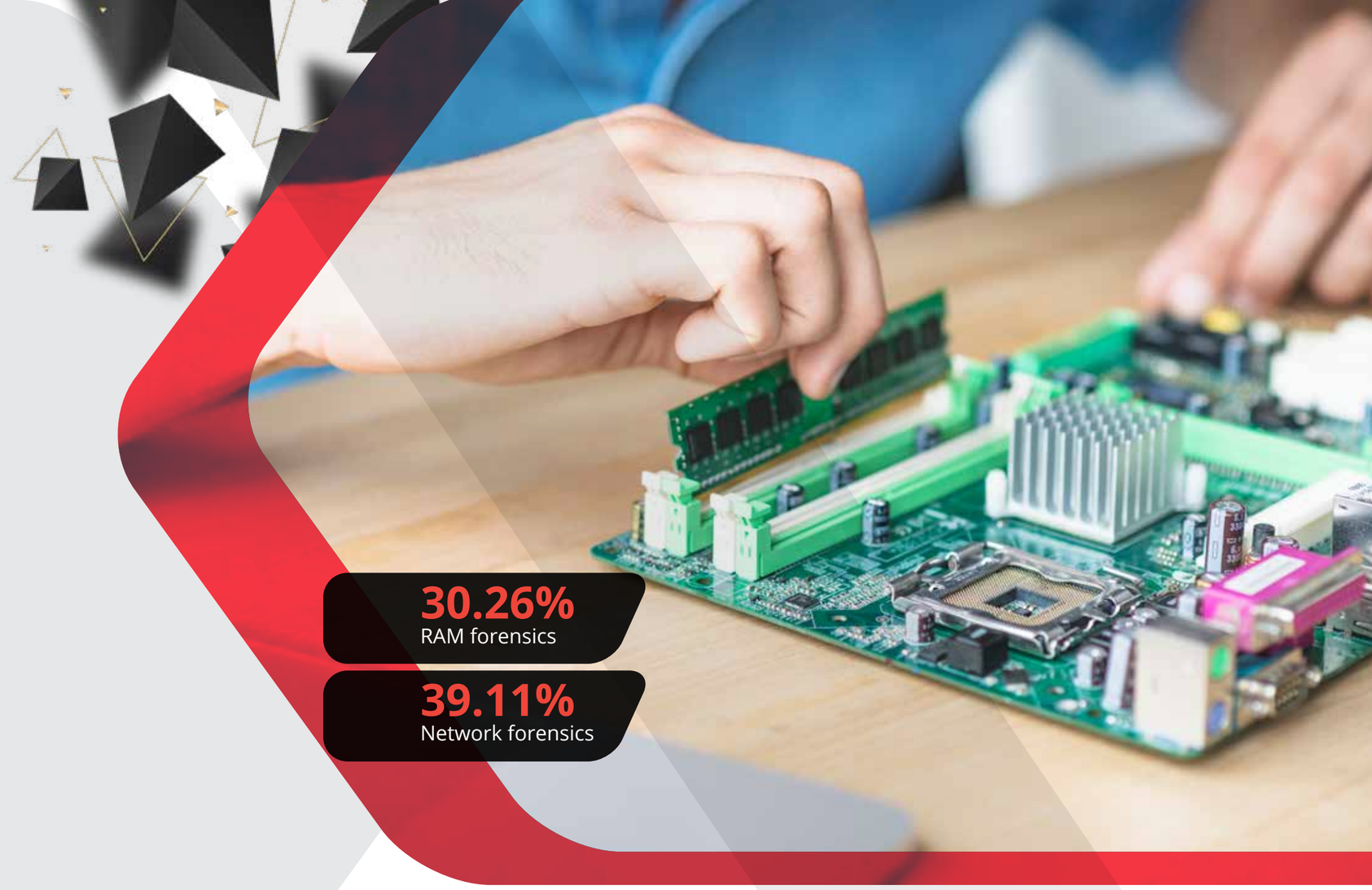
SURVEY

While performing TOR forensics, which of the following forensic techniques would you consider being the most challenging?



30.26%	RAM forensics	6.27%	Hard-disk forensics
23.25%	Registry forensics	1.11%	Other
39.11%	Network forensics		

Base: 271 respondents.

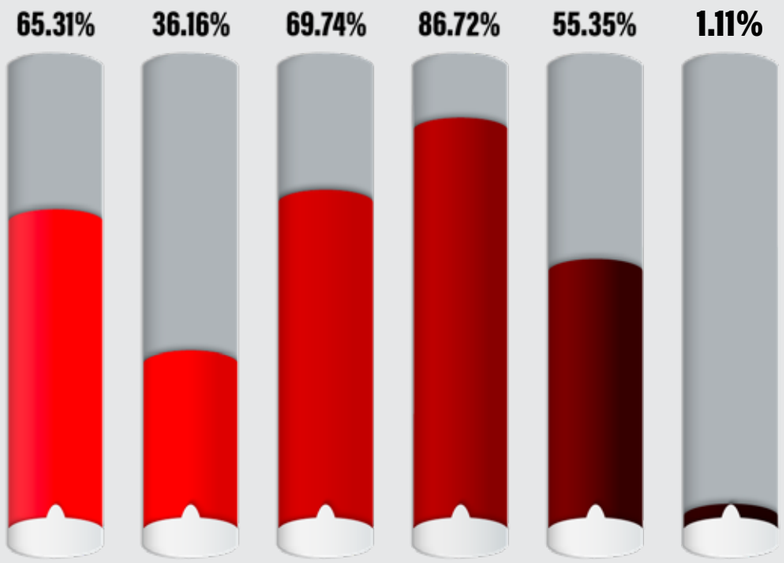


While conducting dark web forensics, the primary element that any digital forensics investigator deals with is a browser such as TOR, Subgraph OS, Waterfox, ISP - Invisible Internet Project, etc., of which TOR is the most widely used browser. Many of the respondents feel that, during analysis, while collecting evidence from TOR, the most challenging part is network traffic forensics (39.11%).

RAM forensics is used to obtain volatile memory from the RAM that will mostly provide evidence related to file types and website browsing history. Both network and database forensics are conducted to get data on the traffic and content, whereas the registry forensics will indicate information related to TOR installation and access. Bitcoin transaction forensics involves extracting artifacts from installed Bitcoin wallet applications on the user's system.

SURVEY

Which techniques do you believe will be widely used in the future to counter anti-forensics techniques?



(More than one option was selected)

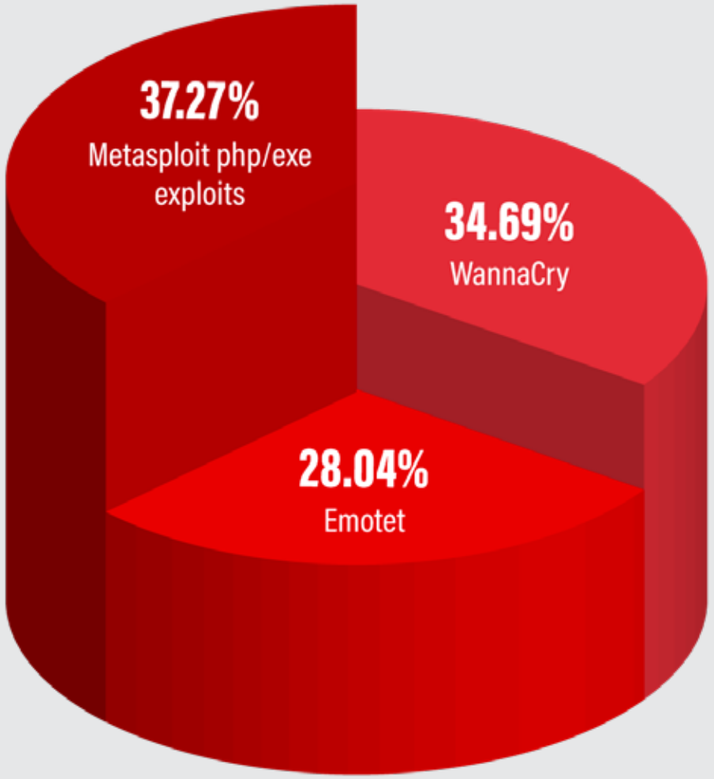
65.31%	File carving	86.72%	Cryptanalysis
36.16%	Password cracking	55.35%	Unpacking program packers
69.74%	Steganalysis	1.11%	Other

Base: 271 respondents.

While digital forensics is the means to counter threats, threat actors are developing and incorporating techniques such as steganography, encryption, packing programs, damaging files, etc., to hide their digital footprint. Many of the respondents believe that amongst the techniques available to counter such anti-forensics techniques, decrypting the encryptions, popularly known as Cryptanalysis (86.72%), will be widely used in the future. This also indicates that an increase in ransomware and data encryption attacks could also be seen.

SURVEY

Which infamous malware and its forensic investigation procedures should DF analysts be aware of as a part of forensic readiness?

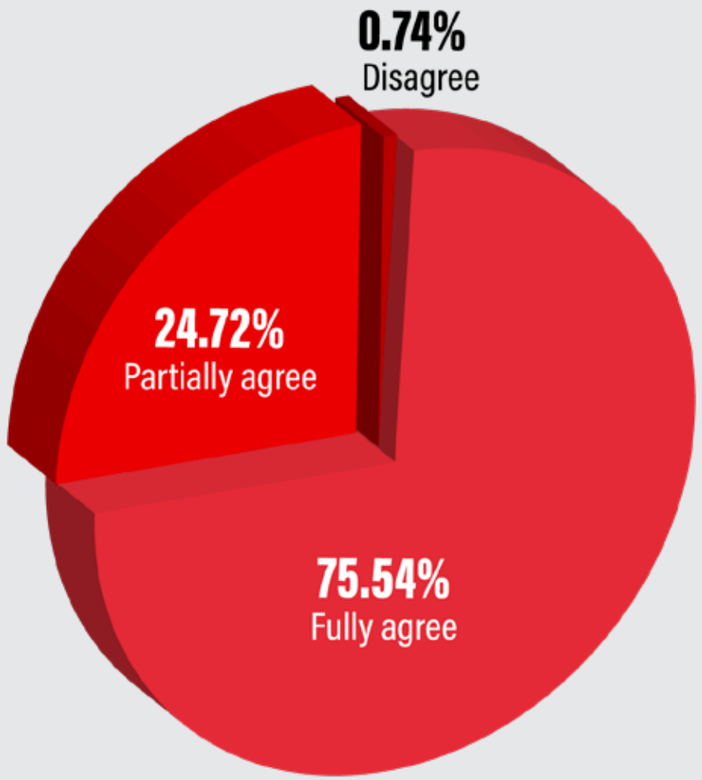


Base: 271 respondents.

Malware is a cause of security breaches in most incidents. Hence, malware forensics is essential for every digital forensic analyst to understand. A majority of the respondents have suggested that Metasploit PHP/Exe exploits are exploited by infamous malware that DF analysts should be aware of, including forensic investigation procedures as part of forensic readiness.

SURVEY

Do you agree that incorporating knowledge of forensics readiness into digital forensics certifications should be mandated?



Base: 271 respondents.

Digital forensics readiness is the ability of an organization to quickly respond to an incident and carry out the forensics investigation. This involves establishing protocols and quickly collecting digital evidence with minimal cost or interruption of the business process. These skills are generally not taught during the DF programs and are said to be acquirable through experience. But a majority of the survey respondents fully agree with the suggestion that forensics readiness should be incorporated into DF certifications and be mandated.

Conclusion

The survey was designed to understand the state of digital forensics in emerging technologies and the challenges posed to it, both in existing and upcoming technologies. The survey was able to provide new insights into how all these aspects could impact and guide the current digital forensics readiness and education to a direction of understanding the existing challenges and developing possible solutions (see Key Findings).

This survey not only highlights the challenges of incorporating digital forensics in emerging technologies such as IoT, cloud, etc., but also sheds light on the existing branches of digital forensics such as malware forensics, databases forensics, browser forensics, dark web forensics, etc., which are either seeing development in some of their aspects or the overall change due to their implementation into an evolving digital environment.

With new developments in technologies, it has become imperative that digital forensics education programs need to develop their curriculum to include a broader skill set, techniques, and technologies that allow for a much-needed exponential change and development required by an individual pursuing digital forensics.

Thus, to help a student in a more abstract way, digital forensics programs must build a relevant academic architecture around the current curriculum to include the impact of digital forensics on emerging technologies and vice versa.

KNOWLEDGE HUB

Beware of the Return to Office: How Organizations Can Protect Against Pandemic Sleeper Threats

Rick Vanover
Senior Director of Product Strategy
Veeam Software

Dave Russell
Vice President of Enterprise Strategy
Veeam Software

As organizations get closer to implementing return-to-work plans, most employees are excited about getting back into an office routine. They miss their colleagues, their favorite lunch spots, and the on-site corporate culture that cannot be replicated over Zoom.

IT administrators have a slightly different view. They miss all the in-office benefits, too, but for them, the prospect of having employees all get back on the network after a year of remote working is a scary thought.

The admins worry that, after a period of being lax about security, employees will bring compromised devices back to the office and expose the company to new threats.

They may have a point. Work computers have played many roles during the pandemic – hosting everything from social gatherings to workouts, online learning sessions, home shopping, and Netflix streams. Family members have borrowed Mom's computer to play online games, and passwords have been passed around. Cyber diligence has taken on a lower priority than it should have. Cybercriminals are well-aware of how insecure employee environments have been. They struck with a round of phishing attacks during the spring 2020 lockdown period. Now, administrators are concerned that hackers might implant vulnerabilities in unsecure laptops and unleash them once employees reconnect with a wider array of resources inside the corporate network.

Some companies did a good job getting ahead of security threats. When remote working became standard practice, some were able to issue company standard devices with regularly patched antivirus security. But the majority found themselves scrambling to enable quick and adequate work-from-home setups that didn't require regular updates, patches, and security checks.

A cybersecurity survey conducted in February reflects just how unprepared enterprises appear to be for the return-to-work security threat. Of those surveyed, 61% used their personal devices – not work-

issued computers – at home. Only 9% used an employer-issued antivirus solution, and only 51% received IT support services while transitioning to remote workstations.

Administrators are bracing for trouble. They're bringing large numbers of potentially unsecured devices back into the fold at the same time they're preparing to accommodate a new normal based on hybrid home/office staffing. According to Veeam's Data Protection Report, 89% of organizations increased their cloud services usage significantly as a result of remote work, and the trend is expected to continue, meaning there will be more endpoints to protect.

So, how can organizations prepare for this transition? Here are a few steps they can take:

Undergo rigorous return-to-work preparation

This is essentially the step where IT administrators physically go through all the affected resources and ensure they're ready to re-enter the game.

Start by carrying out risk assessments for each employee and each device. Which devices have been patched and regularly maintained? Computers used for remote working are likely to have confidential company data on them; where has the company data been saved, and under which account? These checks need to be performed to minimize risk and make sure compliance standards like General Data Protection Regulation (GDPR) are being maintained.

Also, check to see if employees have given away passwords to family members using work computers. Did employees change their passwords? Did they use the same passwords across work accounts and personal accounts? Did they install any new software or remove any during the remote work period? Administrators need to know before they let employees back on their networks.

Next, ensure you scan all relevant devices for unauthorized apps and software. Employees needed to get creative with work solutions, so they may have tapped resources that help them get through everyday tasks but aren't up to security standards. **Run endpoint detection** scans on all returning devices to uncover any hidden vulnerabilities. Cybercriminals often target endpoints, so IT teams need to scan all corporate and personal employee devices that will be brought back to the network.

Improve employees' digital hygiene

While employees may have let their proverbial hair down during remote work, they'll need to rededicate themselves to proper digital hygiene. Push them to use separate

passwords for home and work devices. And make sure they're using conventions that are complex and hard-to-crack. Bring back regular training to ensure that they'll be able to spot phishing emails and other threats. Set up guidelines for using public Wi-Fi and for downloading materials. As employees return to work, it's up to the administrators to refine IT practices, one by one, to protect against the top threats in the organization.

Monitor all activities

The best way to spot problems is to set up a system to flag them as they happen. This practice can be applied to workers' tools – and behaviors – as they reintegrate themselves with all the company's applications. Take advantage of monitoring tools that track changes in usage and applications. If an employee makes a change in an application, you'll want to know. It could be a bug altering a piece of code. Or it could be a change that you made – purposefully or inadvertently – that you'll want to reset. Get in the habit of checking your monitoring tools at least a couple of times a day. It takes a minute, but it allows you to continually reassess your cybersecurity footprint.

Ensure cloud data management and backups are sound

This is a time for IT administrators to make sure all data management and backup services are in good order. If a rogue device does put any data at risk, you'll want to make sure to have backups in service and programmed with practices that will ensure that the data in question is protected and fully available. Keeping the so-called "3-2-1 rule" in mind: Make sure to maintain at least three copies of business data, store critical business data on at least **two** different types of storage media, and keep one copy of the backups in an off-site location. To that, in the ransomware era, we'd expand 3-2-1 to 3-2-1-1-0: Adding another one to the rule where one of the media is offline and ensuring that all recoverability solutions have zero errors.

Conclusion

While IT administrators are looking forward to water-cooler talk and on-site collaboration as much as anybody else, they're understandably concerned about the cybersecurity implications of a more broad-based return to work. It could be a challenge. But with proper planning and follow-through, enterprises can manage the risk and solidify their strategies for protection going forward.

Disclaimer

Views expressed in this article are personal. The facts, opinions, and language in the article do not reflect the views of CISO MAG and CISO MAG does not assume any responsibility or liability for the same.

About the Authors

Rick Vanover (Cisco Champion, VMware vExpert) is Senior Director of Product Strategy for Veeam Software based in Columbus, Ohio. Vanover's experience includes system administration and IT management; with virtualization, cloud, and storage technologies being the central theme of his career recently. As a blogger, podcaster, and active member of the IT community, Vanover builds relationships and spreads excitement about Veeam solutions. Before becoming the "go-to" guy for Veeam questions, Vanover was in system administration and IT management. His community designations include VMware vExpert and Cisco Champion.

Dave Russell recently joined Veeam as its new Vice President of Enterprise Strategy, responsible for driving strategic product and go-to-market programs, spearheading industry engagement, and evangelizing Veeam's vision for the Hyper-Available Enterprise at key events across the globe, and working with the Executive Leadership team in accelerating the company's growth in the enterprise. Russell most recently held the role of Vice President and Distinguished Analyst at Gartner. His research focus at Gartner was on storage strategies and technologies, with an emphasis on backup/recovery, snapshot and replication, software-defined storage (SDS), and storage management. He was the lead author of the Magic Quadrant for Data Center Backup & Recovery Solutions from 2006 to 2017.

Ritesh Chopra
Director Sales and Field Marketing,
India & SAARC Countries
NortonLifeLock

Mobile Side of Technology Adoption Still Continues to Present a Challenge

India has transformed into a mobile-first economy. The ease of accessibility and cheaper data make smartphone steaming content a primary source of entertainment. Given the transition to remote working, people are well accustomed to new technologies and discover different ways to stay connected. Recent incidents have shown the vulnerabilities individuals and business owners can witness if one is not cautious to protect their data and identity in the digital world.

In an interaction with **Augustin Kurian, Assistant Editor of *CISO MAG***, **Ritesh Chopra, Director Sales and Field Marketing, India & SAARC Countries, NortonLifeLock**, discusses the increasing cyberthreats given the current social apps scams that are making consumers vulnerable.

Chopra is responsible for developing and implementing strategies to drive the adoption of NortonLifelock products among consumers in the sub-continent. He champions NortonLifelock's partner strategy in India and manages OEM/ISP and online channel relationships. Chopra also held the position of Country Manager until June 2018 and has been with the company since 2012. With over 20 years of extensive experience in the technology sector, he is a sales and marketing strategist in India and Asia-Pacific regions. He has been recognized with Six Sigma qualification and has successfully conceptualized and implemented multi-tier channel loyalty programs in his previous role with Seagate, Singapore.

In the interview, Chopra provides insights on the growing usage of the dark web and critical findings from the NortonLifeLock Digital Wellness Report.

Email addresses were the most common piece of PII shared with apps and were shared with 48% of the iOS apps and 44% of the Android apps analyzed. With the rise of the dark web, do you think better national cybersecurity regulation can make much difference?

Personally Identifiable Information (PII) such as medical records, bank details, passwords, phone numbers, and email IDs are most targeted by cybercriminals. Cybersecurity regulations will certainly help in making a difference in how data is handled on the dark web. But consumers also need to be aware of the kind of data that is shared through apps. Certain apps can enable attackers to mine information from the device in the background, even without the user's knowledge. Unlike desktop users, smartphone users cannot see the entire URL of the site they are visiting, making them vulnerable to phishing attacks. Such threats can be avoided, to an extent, by using strong passwords, avoiding public WiFi, watching out for phishing emails, regularly backing up important data, and keeping all apps and operating systems up-to-date. Amidst the evolving cybersecurity landscape, it is imperative for individuals to invest in robust anti-theft device security to ensure digital safety.

COVID-19 changed the cybersecurity landscape. It is now even more critical for companies to support the security of their workforce – regardless of geo-location or platform. With myriad compliance and regulations norms varying from country to country, how should a company ensure that best practices are in place across their offices globally?

The COVID-19 pandemic has changed the way we work; the concept of "remote working" is gaining popularity. While people seek opportunities that allow remote work, they must also equip themselves with cyber safety and data protection tools. There are some basic measures you can adopt to avoid falling prey to cyberattacks:

- Speak to your employer to understand the policies that help keep you, your co-workers, and the business safe.
- Always use the company's tech toolbox, as it likely includes firewall and antivirus protection and security features like VPN and two-factor authentication.
- Beware of coronavirus-themed phishing emails used by cybercriminals. Immediately report such phishing attempts to your employer.
- Keep your VPN turned on, as it provides a secure link between employees and businesses by encrypting data. A VPN helps keep information secure from cybercriminals and competitors.
- While working remotely, it is important to understand that online safety is a shared responsibility that begins at the individual level.

> We often download free apps and, often, without thinking, permit them to access different features and data on our device. If something like a weather app asks us to grant access to our contact list, it should give us pause for thought

As far as PCs are concerned, people are increasingly using paid software. They are even adopting security products for Mac machines. But the mobile side continues to present a challenge. We see people adopt VPN and mobile security products; however, it still appears to be a bit further away from what we would want it to be.

India witnessed several state-sponsored attacks during vaccine development. Even the vaccine makers are being targeted in nation-state attacks. What can the country and its cybersecurity divisions do to combat these threat vectors?

Scammers and cybercriminals exploited the COVID-19 pandemic and, more recently, the ongoing vaccination drive, to create new hooks to lure victims. Although the authorities warned people, there has been an enormous increase in the number of phishing scams since the pandemic began. Cybercriminals send emails that appear to be sent by government agencies, employers, and other global health organizations, inviting users to click on what, in reality, are malicious links.

Consumers can adopt some basic measures to falling prey to cyberattacks:

- Beware of online requests for personal information. A coronavirus-themed email that seeks your personal data is likely to be a phishing scam. Legitimate government agencies will not ask for such information. Do not respond to such emails.

- Check the email address or link. You can inspect a link by hovering the cursor over the URL to see where it leads. Sometimes, it is obvious that the web address is not legitimate. Even otherwise, be careful because phishers can create malicious links that closely resemble legitimate addresses.
- Phishing emails are unlikely to address you by your name. Greetings like "Dear Sir or Madam" are an indication that email might not be legitimate.
- Avoid emails that urge you to take immediate action. Phishing emails often try to create a false sense of urgency. The goal is to get the user to click on a link and divulge personal information. If you receive a suspicious-looking email of this type, delete it.

Millennials top the charts in online transactions compared to women and Gen X, who are most complacent about security. Yet, trends indicate Gen X to be more susceptible to cyberattacks than millennials. Do you think it is entirely around digital literacy, or is there more to this trend?

The lines between the virtual and the real world have blurred today. Individuals, irrespective of their age or generation, are vulnerable to cyberattacks when using public or private networks if they do not have any cyber safety solutions installed on their systems. Individuals often neglect to log out of their social media accounts and apps. This habit needs to change. We must bring some good practices from the real world into the virtual one. Akin to how we lock the main door before going to sleep, we should log out of emails and social media accounts, and online banking sessions once we are done using them.

We often download free apps and, usually, without thinking, permit them to access different features and data on our device. If something like a weather app asks us to grant access to our contact list, we should pause for thought. We need to read the terms and conditions carefully too, rather than accepting them blindly. It is advisable to install an application scanner to check for security vulnerabilities and a VPN to mask our identity.

Data from our Digital Wellness Report reveals some interesting facts:

- **81%** of the respondents in the survey were using parental control mechanisms on their devices, while **70%** knew that connecting with strangers while playing online games could lead to problems like cyberbullying.
- The report found that **female respondents (84%) were more aware than men (74%) about security threats and had security software installed on their smartphones**.

- **71%** of female respondents (versus **63%** of male respondents) concerned themselves with app privacy and permissions on their phones.
- **Gen Z** users **(95%)** were found to be more proactive than **millennials (94%)** and **Gen X users (90%)** in adjusting the privacy permissions on their phones.

According to our 2019 NortonLifelock Cyber Insight Report:

- 40% of millennials reported having experienced cybercrime in the past year.
- Nearly 3 in 10 people said they could not detect a phishing attack. Another 13% said they have to guess between a real message and a phishing email. Thus, 4 in every 10 people were vulnerable to phishing.
- 86% of respondents said they may have experienced a phishing incident.
- 7 in 10 respondents wished they could make their home Wi-Fi network more secure.
- 27% of respondents believed it was likely their home Wi-Fi network could be compromised.

At present, fintech is one of the most regulated industries in the world. But the critical challenge is the presence of too many governing bodies but no universal standards – a singular regulatory policy or framework for the industry is lacking. Do you feel there is a need for a standard set of compliance and regulation for fintech and cryptocurrency?

You've probably heard of Bitcoin. But what about Ethereum? Or Tether and Polkadot? What are these? They're all examples of cryptocurrency – a digital currency that you can buy with real money and then spend on online transactions. It's true that you probably can't buy a meal at your favorite restaurant with Bitcoin or rely on Ethereum to fill your car's gas tank. But cryptocurrency is becoming increasingly more popular and valuable. Coindesk.com, which covers cryptocurrency, reported that, as of January 2021, the total value of all cryptocurrencies topped $1 trillion for the first time.

New cryptocurrencies emerge frequently. Coinmarketcap.com listed more than 4,100 types of them in an early 2021 price index published on its site. But what do these digital currencies mean to you? Do you need to learn how to purchase them and spend them? Probably not. But while digital money isn't a necessity, it does have its uses. Users say that digital transactions closed with cryptocurrency are more secure than those using credit cards. As cryptocurrencies become popular, so do the scams associated with them. Some scammers set up fake cryptocurrency exchanges. You might send real money to buy Bitcoins that don't exist. Once you send your funds, they are gone, and your crypto wallet remains empty.

To avoid such scams, only buy cryptocurrency from reputed exchanges. Don't do business with exchanges that seemingly pop up out of nowhere.

What kinds of changes should be made during vendor sourcing and onboarding processes? And how much of the responsibility must fall on the CISO?

Data beaches have a direct negative impact on at least three fundamental aspects of a brand: presence, affinity, and trust. In the age of social media, negative news can affect people's perceptions about the company and the company's financial prospects. Customers might stop engaging with the brand entirely or engage at a significantly lower level than before.

Data security has, for long, been viewed as a "hygiene" factor by many businesses and consumers. However, in today's interconnected world, where data is more valuable than ever and a company's reputation is based on its ability to protect customer data and establish digital trust, cyber safety, and data security are no longer a mere hygiene exercise, but a business differentiator.

There are no set rules for building a security framework, and no system can guarantee 100% protection against all threats. However, imbibing a culture of security within the organization and ensuring the independence and empowerment of the CISO indicates that the organization is serious about cyber safety and data security. It also ensures that critical security-related changes within the organization can be effectively taken care of by the CISO.

About the Interviewer

Augustin Kurian the Assistant Editor of CISO MAG. He writes interviews and features.

REWIND

TOP CYBERSECURITY NEWS OF THE MONTH

THREATS

Twitter's Latest Feature "Tip Jar" Draws Privacy Concerns

On May 6, Twitter added a new feature, the ***Tip Jar***. The intent behind this innovation, as Twitter says, "*is to support voices of creators, journalists, experts, and nonprofits.*" However, within hours of the launch, security experts raised concerns over the privacy of people sending the tips, which according to Twitter's policies seemed like a violation.

What is Twitter's Tip Jar?

Tip Jar allows the Twitterati to generate an additional income source directly via the social media platform. It is a new way of sending and receiving tips so that people can support each other not only in terms of Follows, Retweets, and Likes but even monetarily.

How to enable Twitter's Tip Jar

Setting up the Tip Jar feature is just a matter of few clicks. Follow these simple steps:

- Go to the ***Edit Profile***
- Switch ***On*** the "Tip Jar" setting.
- Toggle and activate ***Allow Tips***. This will display a list of all payment services and platforms available for setting up your tip receiving account.
- Select one or multiple services and add a ***$Cashtag***.
- Once done, the ***Tip Jar*** account for your profile is successfully set up and a small button appears on the profile next to the "Follow" button.

How to send a tip using Tip Jar?

Users can send or donate a tip using Tip Jar by:

- Click on the ***Tip Jar.***
- Select the payment service which you want to send money from (eg. ***Bandcamp, Cash App, Patreon, PayPal,*** and ***Venmo***. Additionally, on Android, tips can also be sent using ***Spaces***).
- Once selected, a Tip Jar prompt appears indicating that the tipper will be redirected to a third-party service outside the platform. Click ***Continue***.
- Go to the platform and complete your payment.

Twitter's Tip Jar Privacy Issue

Though Twitter seems to have nailed this function, some privacy advocates stated that it was exposing the tipper's identity under certain scenarios.

Problem 1: Security researcher Rachel Tobac found out that while sending someone money via PayPal, it revealed her home address to the receiver.

Problem 2: Former Federal Trade Commission chief technologist, Ashkan Soltani, also dug deeper and found that using PayPal for the Tip Jar not revealed users' addresses but even their email addresses, although no transaction took place.

Following these discoveries, Twitter quickly worked around the problem and noticed that the privacy issue was not at their end but the third-party i.e. at PayPal's end. After working out the permutations, they decided that they cannot change PayPal's functionality but update its notification process. Twitter's support handle backed this by tweeting.

"We're updating our tipping prompt and Help Center to make it clearer that other apps may share info between people sending/receiving tips, per their terms."

The Real Problem

On the other hand, PayPal, in its terms and conditions, has already mentioned under which scenarios will the receiver get the address in the receipt. When people are receiving payments through the platform, they need to either select a "goods and services" or "friends and family" payment. In the case of the former, their address is shared, and in the other case, it is not.

THREATS

Snip3: A New Crypter-as-a-Service that Deploys Multiple RATs

Microsoft discovered a spear-phishing campaign in the wild targeting airline, cargo, and travel industries with multiple Remote Access Trojans (RATs). The technology giant stated that attackers distributed malware payloads via phishing emails imitating legitimate businesses with malicious image and PDF attachments.

"The campaign uses emails that spoof legitimate organizations, with lures relevant to aviation, travel, or cargo. An image posing as a PDF file contains an embedded link (typically abusing legitimate web services) that downloads a malicious VBScript, which drops the RAT payloads," Microsoft said.

Stealthy Malware Loader

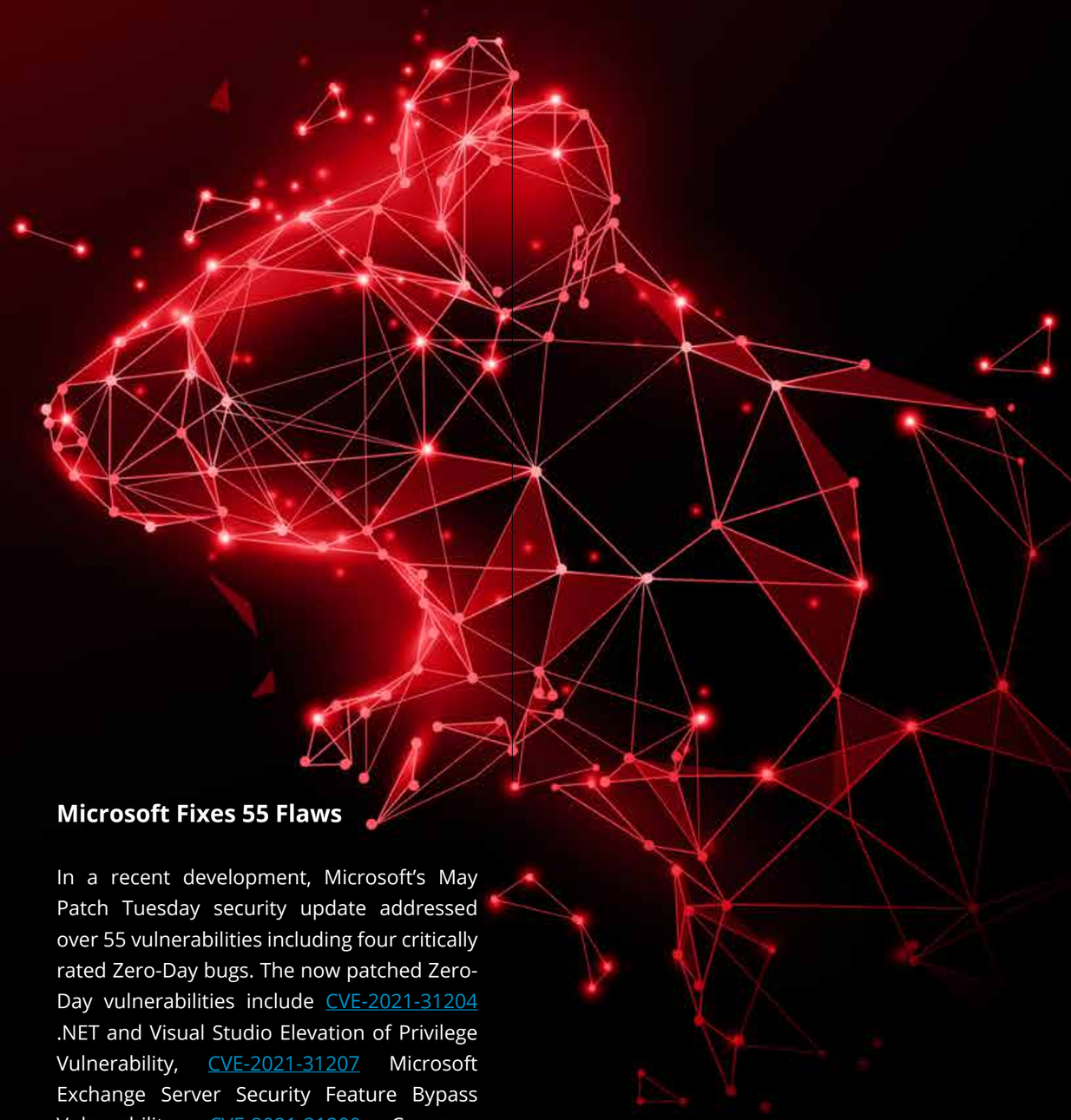
Threat actors leverage multiple RATs to exfiltrate sensitive data from critical systems by adding extra malware payloads. According to cybersecurity firm Morphisec, RATs are delivered via a new and stealthy malware loader **Crypter-as-a-Service** that spreads them onto targeted machines.

The Crypter-as-a-Service, dubbed **"Snip3,"** is used to deploy **Revenge RAT, Agent Tesla, AsyncRAT,** and **NetWire RAT** payloads on compromised systems. Snip3 implements several advanced techniques to bypass detection, such as:

- Executing PowerShell code with the Remotesigned parameter
- Validating the existence of Windows Sandbox and VMWare virtualization
- Using Pastebin and top4top for staging
- Compiling RunPE loaders on the endpoint in runtime

Once the malicious attachment is downloaded, the first-stage VBScript VBS files will be installed simultaneously executing the second-stage PowerShell script, which in turn executes the final RAT payload using Process Hollowing.

"The Snip3 Crypter's ability to identify sandboxing and virtual environments make it especially capable of bypassing detection-centric solutions. As a result, organizations with detection-focused stacks need to be wary of attacks like Snip3 and others. Morphisec customers can rest easy that they are protected against the evasive techniques Snip3 and other attacks like it employ," Morphisec said.



Microsoft Fixes 55 Flaws

In a recent development, Microsoft's May Patch Tuesday security update addressed over 55 vulnerabilities including four critically rated Zero-Day bugs. The now patched Zero-Day vulnerabilities include CVE-2021-31204 .NET and Visual Studio Elevation of Privilege Vulnerability, CVE-2021-31207 Microsoft Exchange Server Security Feature Bypass Vulnerability, CVE-2021-31200 Common Utilities Remote Code Execution Vulnerability, and Zero Day Initiative flagged CVE-2021-31166.

CYBER ATTACKS

Irish Health Services Shut Down After Being Hit by Ransomware Attack

Ireland's health care services were temporarily disrupted after being hit by a ransomware attack. The Irish Health Service Executive (HSE) claimed that the attack affected several diagnostic services, disrupted COVID-19 testing operations, and forced hospitals to cancel many medical emergencies.

Zero-Day Attack!

According to Ossian Smyth, Ireland's minister of e-government and head of the HSE, an international cybercriminal gang is behind the attack. It was found that the attackers exploited an unknown vulnerability in the IT systems that led to a Zero-Day attack, affecting IT systems services at all local and national health care facilities. While the attack may potentially affect sensitive information stored on central servers, health care officials stated that there was no sign of misuse of any patient data or connected medical equipment.

"These are cybercriminal gangs, looking for money. What they're attempting to do is to encrypt and lock away our data, and then to try to ransom it back to us for money. It's widespread. It is very significant, and possibly the most significant cybercrime attack on the Irish State," Smyth said.

Patients – The Primary Victims

The attack primarily affected several patients who needed medical attention as the majority of the hospitals canceled all appointments.

No Ransom!

While there was no sign of any ransom demand from cybercriminal groups, the Prime Minister of Ireland Micheál Martin announced that they will not be going to pay any ransom.

Besides, Ireland's Health Minister Stephen Donnelly stated the attack impacted most health and social care services severely.

Currently, the health care authorities in the country are working on restoring the IT systems to help patients who are in medical need. "We apologize for the inconvenience caused to patients and the public and will give further information as it becomes available. Vaccinations not affected are going ahead as planned," HSE said.

DATA BREACH

Toshiba's European Subsidiary Confirms Ransomware Attack; DarkSide's Involvement Suspected

As the ransomware pandemic ravages through the big and small size industries alike, the Japanese tech giant joins the list of those affected by it. Toshiba's European subsidiaries have confirmed that it was targeted by a "cyberattack". As per the initial investigation, the involvement of the **DarkSide ransomware** gang is being suspected as the malware signatures of this attack are similar to those used in the Colonial pipeline hack.

Toshiba Subsidiary Confirms Ransomware Attack

The European subsidiaries of Toshiba Tec Group on May 14 disclosed information that a cyberattack on their network and systems had meant that the network connections between their company assets in Japan and Europe were taken offline to stop the spread of the malware. A tweet from Toshiba's French subsidiary, Tec France Imaging System (TFIS), confirmed that it was indeed a ransomware attack and took place on the night of May 4.

The official statement made by the Toshiba Tec Group said that the investigation was ongoing and only "some regions in Europe" were affected by the attack. It further added that until now, there was no information available that could pinpoint the fact that customer-related information was leaked externally during the course of the attack. However, it has not entirely ruled out the possibility of the leak either. It said, "The group recognizes that it is possible that some information and data may have been leaked by the criminal gang, we will continue to conduct further investigation in cooperation with the external specialized organization to grasp the details."

DarkSide's Involvement

Nowhere in its statement or on official channels did Toshiba Tec Group name the DarkSide ransomware gang's hand in the attack. But in a report from ***CNBC***, a Toshiba spokesperson said that the DarkSide criminal group appeared to be responsible for the security incident. However, the spokesperson confirmed that it did not intend to pay the ransom and instead used its data backup procedures to get the systems and networks back online.

DATA BREACH

Personal Data of 4.5 Mn Passengers Exposed in Air India Data Breach

While most flight passengers want to make their air travel hassle-free during the pandemic, the growing cyberattacks on the aviation industry have become a challenge for several airlines. Travelers are skeptical and cautious about sharing their personal information with airlines in the wake of heightened security breaches.

Recently, India's national airline Air India revealed that it sustained a sophisticated data breach in February 2021, which affected over 4.5 million passengers globally, after its data management service provider SITA Passenger Service System (SITA PSS) was hacked by unknown threat actors. SITA PSS is responsible for storing and processing of personal information of Air India passengers. "While we had received the first notification in this regard from our data processor on February 25, 2021, we would like to clarify that the identity of the affected data subjects was only provided to us by our data processor on March 25 and April 05, 2021. The present communication is an effort to apprise of accurate state of facts as on date and to supplement our general announcement of March 19, 2021, initially made via our website," Air India said.

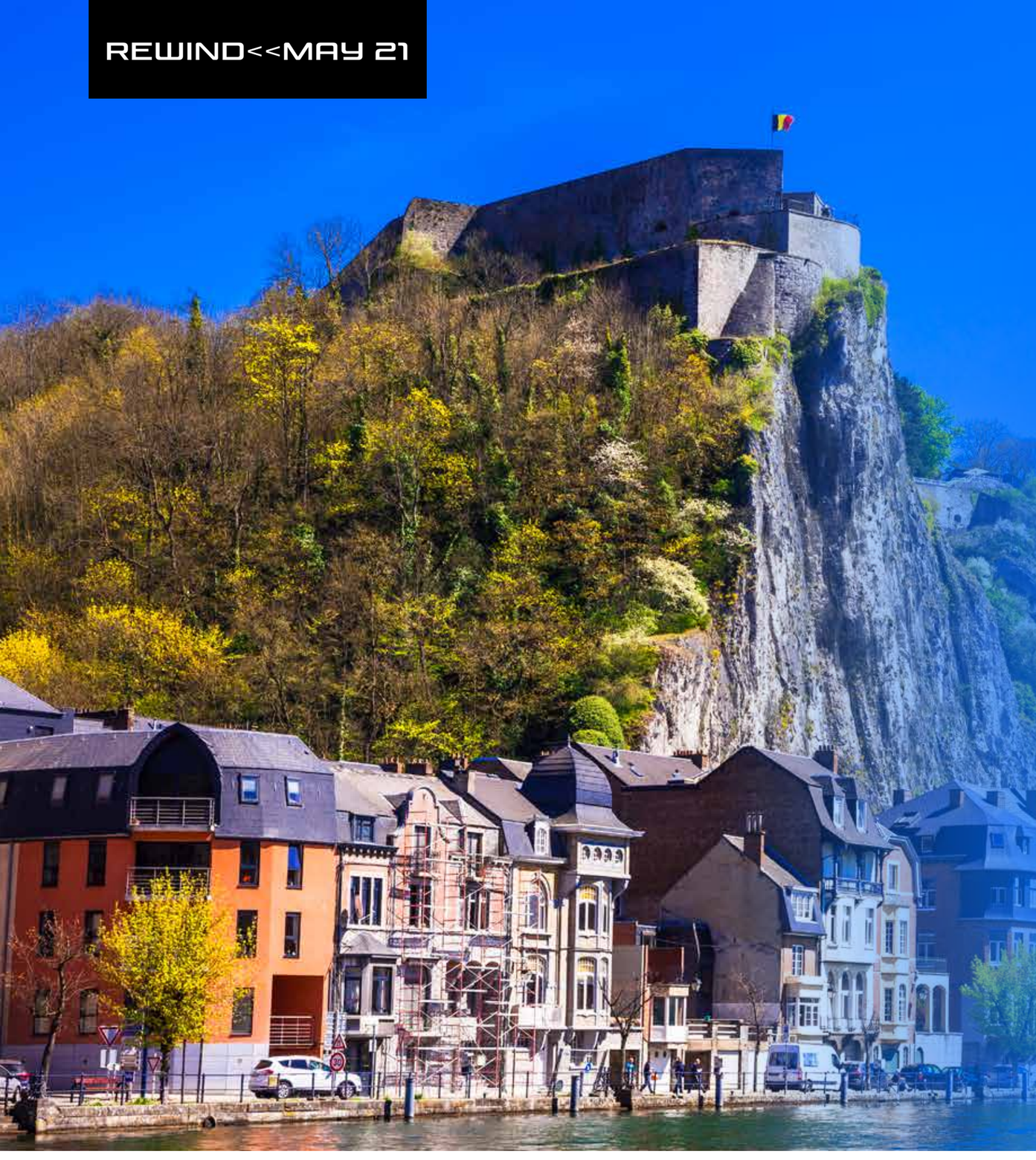
A Decade Worth of Passenger Data

Air India stated the data breach affected passengers who had registered between August 26, 2011 and February 3, 2021. It was found that the attackers managed to access a decade worth of passenger data including names, passport, credit card details, birth dates, contact information, passport information, ticket information, and Air India's frequent flyer data from SITA's systems. However, the company clarified that CVV/CVC numbers were not exposed in the incident.

Measures Taken by Air India After the Data Breach:

- Investigating the data security incident
- Securing the compromised servers
- Engaging external specialists of data security incidents
- Notifying and liaising with the credit card issuers
- Resetting passwords of the Air India FFP program

While there is no sign of any misuse of users' leaked data, Air India urged passengers to update their passwords at the earliest to avoid any security risks.



GOVERNANCE

Belgium's National Security Council Approves Cybersecurity Strategy 2.0

At the beginning of the month, Belgium faced a widespread internet outage across the country. Reportedly, the country's leading internet service provider (ISP), Belnet, was targeted with multiple waves of DDoS attacks that forced nearly 200 organizations, including government websites, to go offline. Incidentally, around the same time, Belgium's National Security Council (NVR) was finalizing the country's **Cybersecurity Strategy 2.0**, whose first version was introduced in 2012 and implemented in the preceding year. The original strategy, which contains 11 of the 15 strategic goals of the European Union Agency for Cybersecurity (ENISA), has been renewed to add six more specific areas that it will concentrate on in the next five years.

Cybersecurity Strategy 2.0: Six Strategic Areas of Focus

Belgium's various industrial sectors and even SMEs are taking huge strides towards cutting-edge technological adoptions. The country's cyberspace is continuously evolving and thus the challenges that come with it have evolved too. However, the country has always paid attention to this and invested in securing its cyber front. Cybersecurity is one of the main pillars of their National Plan for Recovery and Resilience, which the government submitted to the European Commission at the end of April.

Cyberthreats are dynamic and require evolving countermeasures. Thus, to take its cyber defenses a notch higher, Belgium's National Security Council has approved adding and adopting a new and more refined cybersecurity strategy based on six specific objectives:

- Strengthen the digital environment and confidence in it.
- Protect the computers and networks of both, end-users and service providers.
- Protect critical organizations from cyberthreats.
- Raise awareness and educate all stakeholders to tackle all possible cyberthreats.
- Improve partnerships and sharing of expertise between government, industry, and academic institutions.
- Make a clear international commitment concerning cybersecurity.

The CCB will work closely with various government services for which cybersecurity is of central importance.

GOVERNANCE

Japan to Impose Strict Regulations on Private Sector's Adoption of Foreign Equipment and Technology

Fearing a situation like the Colonial Pipeline-like hack, the Japanese government is set to impose restrictions on the usage of foreign equipment and technology in its private sector. It will introduce new security regulations for 14 critical infrastructure sectors including, telecommunications, electricity, finance, railroads, government services, and health care.

The Policy in Public Sector

Japan had reportedly stopped procuring foreign equipment in government purchases since 2018 "to avoid hacks and intelligence leaks." The move was specifically aimed at keeping China at bay, who at the time were being blamed by the U.S. for carrying out spying and espionage campaigns through Huawei's 5G equipment. Following these accusations, the U.S., the U.K., and Australia ordered an immediate ban on importing Huawei's 5G equipment and ordered the removal and replacement of the installed equipment too. Japan being a close ally of the U.S., and the fact that it could cause economic security risks to its homeland, followed suit.

However, the recent turn of events in the U.S., where the privately run Colonial Pipelines was hacked, probably pressured the Japanese government into extending this ban to the private sector too. The brutal ransomware attack on the Colonial Pipeline infrastructure saw a temporary halt in its supplies affecting many major East Coast cities including Washington, DC., Baltimore and Atlanta. Concerns over a fuel crunch and price hike saw frantic buying from citizens of these regions, which further escalated the fuel shortage. The situation was later brought under control as a partial recovery of fuel supplies was attained soon. The chaos led to the POTUS signing an Executive Order to bolster the nation's fight against rising cyberattacks.

Present Private Sector Woes

In the same week, another Japanese tech giant Toshiba's subsidiary in Europe fell victim to a ransomware attack, which was probably conducted by the same threat group involved in the Colonial Pipeline hack. The attack led to the suspension of all communication lines between Toshiba's European and Japanese offices.

STAY VISIBLE!

REACH OUT TO THE EVER GROWING GLOBAL INFOSEC COMMUNITY

ADVERTISE WITH US

CISO MAG
beyond cybersecurity

FOR MORE INFO WRITE TO
cisomag@eccouncil.org

230,000
Readership Reach
EC-Council & CISO MAG Combined

30,000+
Registered Readership
EC-Council & CISO MAG Combined

90,000
New Page Views

cisomag.eccouncil.org

CISO MAG

beyond cybersecurity

SCAN AND STAY UPDATED WITH
REAL TIME CYBERSECURITY NEWS