CYBERSECURITY: EMERGING THREATS AND MITIGATION STRATEGIES

Gogwim, Joel Godwin, B. Tech (Hons), MPhil. (SA), CCNA, CCDA, CCAI, CCNP, CCDP, CEH, MNCS, MCPN, MNiRA, MCFIN
ICT Directorate University of Jos, Nigeria
email: gogwim[at]unijos.edu.ng
Skype ID: gogwim

Introduction

Cybersecurity is the process of preventing, defending, and protecting Internet-connected systems, including hardware, networks devices, software, applications and data, from cyber attacks. In a computing context, security comprises cyber security and physical security of infrastructure - both are used by enterprises to protect against unauthorized access to data centres and other computerized systems.

The revolution of the Internet and its affordances had induced organizations and government globally to pivot toward a digital operations or business model; and in the process a lot of data is exponentially generated and shared among organizations, partners and customers. It is important to note that this digital information has become the lifeblood of the interconnected business ecosystem and is increasingly valuable to organizations, government, and even to skilled threat actors. This has exposed organizations and government to new digital vulnerabilities, making effective cybersecurity and privacy more important than ever.

Global cyber attacks like the one that struck Ukrainian government agencies and international businesses toward the end of June 2017 routinely spur urgent discussion about how to identify and counter the latest bespoke threats. The media narrative on cyber attacks is often episodic and driven by the emerging threats. Headlines frequently feature unusual names for malware intended to distinguish the latest threats from the last. However, management of cyber threats cannot be episodic, thus rather than focusing on the seemingly endless stream of threats, corporate directors, CEOs and other senior personnel should stay focused on business risk. Mitigating cyber risks is like managing any other kind of business risk – it requires tradeoffs. It comes down to proactively aligning resources to mitigate the likelihood of cybersecurity incidents and limit the damage when some cyber attacks inevitably penetrate defenses.
The cyber threat landscape continues to evolve, with new threats emerging almost daily. The ability to track and prepare to face these threats can help security and risk management leaders improve their organization's resilience and better support business goals.

Emerging Threats
Outline are emerging cybersecurity threats that business, technology, government and security leaders need to pay attention to with potential mitigation strategies to help deter the evolving methods of cyber-criminals.

1. ATM “Jackpotting”—There have been reports of ATM “black box”-style attacks, in which cyber-criminals attach a hard drive or laptop to the ATM, displacing the current ATM software. Once the ATM is running off the malware-infected hard drive, it can be remotely controlled to dispense cash on demand. While these physical ATM attacks have been happening in Europe and Asia since 2012, they are new to the U.S. and some African countries as of last year.

2. Malware-only ATM Attacks—In addition to the black-box “jackpotting” schemes, which require internal, physical access to internals to the ATM itself, there have also been network-based ATM attacks in other parts of the world since 2016. In general, the attackers were able to gain access to a bank’s internal network through the usual probing mechanisms (spearphishing, social engineering, etc.), and then navigate the bank’s internal networks to deploy malware out to the ATMs. The cyber-criminals could then remotely control the infected ATM to dispense cash on demand. This style of ATM attack has not hit the Africa yet, but it is an emerging threat financial services’ senior management needs to be aware of. Like the ATM “black box,” it could be a tactic used in the Africa sooner rather than later.

3. Endpoint vulnerabilities - Another prevalent and evolving, if not fully emerging threat that needs to be monitored and addressed is end-user PC and laptop vulnerabilities; these are constant security risk. The reason these “endpoints” are
so important for cybersecurity is they site at the beginning of the vulnerability and compromise. When cyber-criminals send their phishing email or their malicious attachments to a company’s employees, what they are targeting is any device that can be exploited to obtain access to the network. This is the first point of compromise for a cyber-attack, establishing a beachfront for further malicious activities. By being better able to ward off endpoint attacks, financial institutions will prevent more complex threats from progressing. Protecting the endpoints is a core part of the cybersecurity puzzle that your team should be very aware of.

4. **Biometric Hacking** - Many IT professionals are incorporating more biometric data in their authentication processes, and the approach does seem to be the most secure. All of our thumbprints are unique, after all. But hackers have already proven once again that where there’s a will, there’s a way. “You can actually 3D print a replica of someone’s face to fool facial recognition technology,” said Michael Bruemmer, vice president of Experian’s data breach resolution group. Some Android phones have unlocked when shown a simple photograph of their owners’ faces. Scans of facial features and fingerprints are also stored and can be stolen the same as a typed password or numerical code. As many as 5.6 million fingerprints were stolen in 2015. An increasing number of facilities and police forces are also using facial recognition technology for security purposes. “Most people don’t realize how much biometrics affect daily life,” Bruemmer said. It’s in the airport check-in process, employers use it to track time and attendance, and law enforcement uses it. Almost all of our devices use some form of biometric confirmation.

5. **Gaming as a Cyber Attack Launch Pad** - Online gaming has soared in popularity over the past few years. About one-quarter of the world’s populations are gamers. According to Statista, free-to-play and pay-to-play massively multiplayer online (MMO) gaming generated roughly $19.9 billion in 2016, and the data volume of global online gaming traffic is forecast to grow from 126 petabytes in 2016 to 568 petabytes in 2020. Gamers are comfortable with the dark web, they have great computer skills, and they operate anonymously. So it stands to reason that they have the skills and the motivation to hack into other games in
order to steal valuable data like credit card information or other data or identity. Late last year, the browser-based game Town of Salem suffered such a breach that went unnoticed for days while employees were away on holiday break. Stolen data included email addresses, usernames, IP addresses, game-related activity, passwords and payment information.

6. **Multi-Vector Dark Web Attacks** - Phishing emails, malware-infected links and theft of authentication information are still cyber security risks to watch. But after a multitude of attacks and lessons learned, security teams do have the tools and systems in place to mitigate these types of attacks. The attack we’re not ready for is the one that turns our own devices against us. Wannabe cyber criminals can easily purchase botnet installation software on the dark web. Botnets are connected computers that work together to perform a task and are always running in the background to keep websites updating. But run by a malicious hacker, they can be used to take over your computer. Essentially, multi-vector attacks turn your device into a foot soldier for the enemy. This provides an exponentially larger attack surface for cyber thieves to collect data. Nowadays, you don’t have to be technologically sophisticated to carry out an attack like this. You can buy kits on the dark web and follow the instructions to install malware, or hack into Bluetooth, or spoof a free public WiFi spot. This allows people with very little computer literacy to get into the game of stealing information.

7. **Cryptojacking** - Ransomware has been one of the biggest threats impacting businesses in the past two years, exploiting basic vulnerabilities including lack of network segmentation and backups, Gartner's Olyaei said. Today, threat actors are employing the same variants of ransomware previously used to encrypt data to ransom an organization's resources or systems to mine for cryptocurrency -- a practice known as cryptojacking or cryptomining.

8. **Internet of Things (IoT) device threats** - Companies are adding more and more devices to their infrastructures, said Forrester's Zelonis. "Organizations are going and adding solutions like security cameras and smart container ships, and a lot of these devices don't have how you're going to manage them factored into the design of the products." Maintenance is often the last consideration when it comes
to IoT, Zelonis said. Organizations that want to stay safe should require that all IoT devices be manageable and implement a process for updating them.

9. **Geopolitical risks** - More organizations are starting to consider where their products are based or implemented and where their data is stored, in terms of cybersecurity risks and regulations, Olyaei said. "When you have regulations like EU General Data Protection Regulation (GDPR) and threat actors that emerge from nation states like Russia, China, North Korea, and Iran, more and more organizations are beginning to evaluate the intricacies of the security controls of their vendors and their suppliers," Olyaei said. "They're looking at geopolitical risk as a cyber risk, whereas in the past geopolitical was sort of a separate risk function, belonging in enterprise risk. If organizations do not consider location and geopolitical risk, those that store data in a third party or a nation state that is very sensitive will run the risk of threat actors or nation state resources being used against them. If you do that then you also impact the business outcome.

10. **Cross-site scripting** - Organizations struggle to avoid cross-site scripting (XSS) attacks in the development cycle, Zelonis said. More than 21 percent of vulnerabilities identified by bug bounty programs are XSS areas, making them the leading vulnerability type, Forrester research found. XSS attacks allow adversaries to use business websites to execute untrusted code in a victim's browser, making it easy for a criminal to interact with a user and steal their cookie information used for authentication to hijack the site without any credentials, Forrester said. Security teams often discount the severity of this attack, Zelonis said. But bug bounty programs can help identify XSS attacks and other weaknesses in your systems, he added.

11. **Mobile malware** - Mobile devices are increasingly a top attack target -- a trend rooted in poor vulnerability management, according to Forrester. But the analyst firm said many organizations that try to deploy mobile device management (MDM) solutions find that privacy concerns limit adoption. The biggest pain point in this space is the Android installed base, Zelonis said. "The Google developer site shows that the vast majority of Android devices in the world are running pretty old versions of Android," he said. And when you look at the
Motivations of a lot of IoT device manufacturers, it's challenging to get them to continue to support devices and get timely patches, because then you're getting back to mobile issues. Organizations should ensure employee access to an anti-malware solution, Forrester recommended. Even if it's not managed by the organization, this will alleviate some security concerns.

Mitigation Strategies

It is important to remember that technology plays a strong role here, as well. Beyond just routine software patching and the standard antivirus software and anti-malware products you are probably already familiar with, there are newer families of next-generation, advanced endpoint-protection products that can help to defend against compromise. The complexity of the threat landscape underscores the need for corporate leaders to embed strong management of cyber and privacy risk management into the fiber of their organizations.

Fortunately, maintaining robust cyber hygiene can help companies mitigate significant risks. It takes committed leadership, however, to put this into action on a continuous basis. Here are a few pragmatic steps that can be taken to better manage these risks:

1. Standalone, kiosk-style ATMs have been the most prone to “black box” style attacks. Making the exterior of the ATM physically harder would offer better protection of the internal components from tampering.

2. To prevent network-based attacks on ATMs, however, network segmentation would be part of a good strategy. It is important to ensure that only legitimate traffic can pass through to critical resources anywhere in your environment. In this case, you want to separate your ATM network from the rest of your corporate IT network, which reduces the risk to that portion of the environment. While the idea of network segmentation for cybersecurity is not new, the adoption of this strategy is starting to pick up and become more prevalent. The trend now is to partition the internal networks and to not trust any traffic but be fully aware of what traffic is flowing through the network, and only allow those applications that are critical for your business.
3. Training and education of employees are a key part of your defense. For instance, employees must be acutely aware of the kind of emails and links they should be wary of. Training about what to look out for and how to respond to malicious attachments or attempts at socially engineering are paramount.

4. **Strategic assessments of cyber threats and vulnerabilities** - conducting risk assessments that show how creative hackers of different stripes might seek to undermine the organization’s security for various motives, and where security gaps exist, enabling the C-suite to better align resources to counter the most significant cyber risks.

5. **Rapidly spotting and countering threats** - strengthening the ability to rapidly identify, detect and contain threats, as well as broadening the sharing of threat data with peers and authorities to provide faster, actionable intelligence capable of driving measurable security improvements.

6. **Robust business continuity planning and exercising** - ensuring that individual user systems and key servers can be restored rapidly from backups, and that the frequency of backups aligns to the timeframe of data your organisation is prepared to lose in the event of any system being rendered unusable.

7. **Crisis and incident response planning and exercising** - ensuring that there are formal procedures in which employees and those responsible for the management of high priority incidents are well versed to streamline the organisation’s reaction to ransomware events and its ability to restore service to employees and customers.

8. **Strong security hygiene policies and user awareness** - preventing ransomware entering your IT environment through the most common delivery vector, phishing, by enforcing strong controls at your email gateways and network perimeters, and developing vigilant employees through robust awareness campaigns.

9. **Rigorous patch and vulnerability management** - the vulnerabilities exploited in the Petya attack have already been addressed via Microsoft ‘critical’ patches released in March 2017. A robust vulnerability management programme will help reduce the likelihood of exploitation.
10. Update and Upgrade Software Immediately Apply all available software updates, automate the process to the extent possible, and use an update service provided directly from the vendor. Automation is necessary because threat actors study patches and create exploits, often soon after a patch is released. These “N-day” exploits can be as damaging as a zero-day. Vendor updates must also be authentic; updates are typically signed and delivered over protected links to assure the integrity of the content. Without rapid and thorough patch application, threat actors can operate inside a defender’s patch cycle.

11. Defend Privileges and Assign privileges based on risk exposure and as required to maintain operations. Use a Privileged Access Management (PAM) solution to automate credential management and fine-grained access control. Another way to manage privilege is through tiered administrative access in which each higher tier provides additional access, but is limited to fewer personnel. Create procedures to securely reset credentials (e.g., passwords, tokens, tickets). Privileged accounts and services must be controlled because threat actors continue to target administrator credentials to access high-value assets, and to move laterally through the network.

12. Enforce Signed Software Execution Policies Use a modern operating system that enforces signed software execution policies for scripts, executables, device drivers, and system firmware. Maintain a list of trusted certificates to prevent and detect the use and injection of illegitimate executables. Execution policies, when used in conjunction with a secure boot capability, can assure system integrity. Application Whitelisting should be used with signed software execution policies to provide greater control. Allowing unsigned software enables threat actors to gain a foothold and establish persistence through embedded malicious code.

13. Exercise a System Recovery Plan Create, review, and exercise a system recovery plan to ensure the restoration of data as part of a comprehensive disaster recovery strategy. The plan must protect critical data, configurations, and logs to ensure continuity of operations due to unexpected events. For additional protection, backups should be encrypted, stored offsite, offline when possible, and support complete recovery and reconstitution of systems and devices. Perform periodic
testing and evaluate the backup plan. Update the plan as necessary to accommodate the ever-changing network environment. A recovery plan is a necessary mitigation for natural disasters as well as malicious threats including ransomware.

14. Actively Manage Systems and Configurations Take inventory of network devices and software. Remove unwanted, unneeded or unexpected hardware and software from the network. Starting from a known baseline reduces the attack surface and establishes control of the operational environment. Thereafter, actively manage devices, applications, operating systems, and security configurations. Active enterprise management ensures that systems can adapt to dynamic threat environments while scaling and streamlining administrative operations.

15. Continuously Hunt for Network Intrusions Take proactive steps to detect, contain, and remove any malicious presence within the network. Enterprise organizations should assume that a compromise has taken place and use dedicated teams to continuously seek out, contain, and remove threat actors within the network. Passive detection mechanisms, such as logs, Security Information and Event Management (SIEM) products, Endpoint Detection and Response (EDR) solutions, and other data analytic capabilities are invaluable tools to find malicious or anomalous behaviors. Active pursuits should also include hunt operations and penetration testing using well documented incident response procedures to address any discovered breaches in security. Establishing proactive steps will transition the organization beyond basic detection methods, enabling real-time threat detection and remediation using a continuous monitoring and mitigation strategy.

16. Leverage Modern Hardware Security Features Use hardware security features like Unified Extensible Firmware Interface (UEFI) Secure Boot, Trusted Platform Module (TPM), and hardware virtualization. Schedule older devices for a hardware refresh. Modern hardware features increase the integrity of the boot process, provide system attestation, and support features for high-risk application containment. Using a modern operating system on outdated hardware results in a
reduced ability to protect the system, critical data, and user credentials from threat actors.

17. Segregate Networks Using Application-Aware Defenses - Segregate critical networks and services. Deploy application-aware network defenses to block improperly formed traffic and restrict content, according to policy and legal authorizations. Traditional intrusion detection based on known-bad signatures is quickly decreasing in effectiveness due to encryption and obfuscation techniques. Threat actors hide malicious actions and remove data over common protocols, making the need for sophisticated, application-aware defensive mechanisms critical for modern network defenses.

18. Integrate Threat Reputation Services Leverage multi-sourced threat reputation services for files, DNS, URLs, IPs, and email addresses. Reputation services assist in the detection and prevention of malicious events and allow for rapid global responses to threats, a reduction of exposure from known threats, and provide access to a much larger threat analysis and tipping capability than an organization can provide on its own. Emerging threats, whether targeted or global campaigns, occur faster than most organizations can handle, resulting in poor coverage of new threats. Multi-source reputation and information sharing services can provide a more timely and effective security posture against dynamic threat actors.

19. Transition to Multi-Factor Authentication Prioritize protection for accounts with elevated privileges, remote access, and/or used on high value assets. Physical token-based authentication systems should be used to supplement knowledge-based factors such as passwords and PINs. Organizations should migrate away from single factor authentication, such as password-based systems, which are subject to poor user choices and susceptible to credential theft, forgery, and reuse across multiple systems.