Ransomware and Cyber Resilience in the Digital Age

Amit Ghodekar & Nicki Doble

This whitepaper discusses recent trends in the cybersecurity sector related to ransomware – both what it is, and how to prevent it – and cyber resilience, as distinct from cyber defense. Analysis is split into two sections - Section A discusses ransomware and is intended for technically minded personnel, Section B deals with cyber resilience and has been written with a broader C-suite audience in mind.

Section 1 - Ransomware: a new evil in the digital age

Author: Amit Ghodekar

Today's security executives have their hands full, monitoring everything from remote endpoint security policies to increased global privacy regulations and ever evolving cyber threats. Ransomware gangs are constantly changing and evolving their tactics to circumvent cybersecurity efforts and maximize pressure on victims to pay the ransom. For example, not too long ago, security experts were issuing warnings about double extortion ransomware threats. Today, ransomware operators have upped the ante by adding triple extortion tactics to the mix. Now, not only do businesses have to worry about malicious data encryption and exfiltration but their customers may also be hit with ransom demands or a DDoS attack if the original victim refuses to pay.

The cost of recovery from successful ransomware attacks is also on the rise. According to The State of Ransomware 2021 report by cybersecurity firm Sophos, the average total cost of recovery from a ransomware attack has more than doubled in the past year from $761,106 in 2020 to $1.85 million in 2021. Today's cyberthreat landscape makes ransomware attacks almost inevitable. Although detection and prevention are IT security teams' top priorities, the reality is that you must be ready with both a proactive defense strategy and a vigorously tested plan to orchestrate recovery.

What is ransomware?

Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. In recent years, ransomware incidents have become increasingly prevalent among the nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations.

Malicious actors continue to adjust and evolve their ransomware tactics over time, and the now it's a time for the Governments, as well as the private sector require to remain vigilant in maintaining awareness of ransomware attacks and associated tactics, techniques, and procedures around the world.

Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. Malicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion. The monetary value of ransom demands has also increased, with some demands exceeding US $1 million. Ransomware incidents have become more destructive and impactful in nature and scope.

Malicious actors engage in lateral movement to target critical data and propagate ransomware across entire networks. These actors also increasingly use tactics, such as deleting system backups, that make restoration and recovery more difficult or infeasible for impacted organizations. The economic and reputational impacts of ransomware incidents, throughout the initial disruption and, at times, extended recovery, have also proven challenging for organizations large and small In the past, criminals demanded ransoms be sent via cash or money order to post office boxes. However, that didn't always last because post office boxes are traceable to an individual. Today, the ransom is almost always requested in the untraceable, anonymous currency of Bitcoin. Now that ransoms can be paid in an untraceable manner, the frequency of ransomware attacks has exploded. Ransomware is new type of Digital Extortion, it should be called out for what it really is – extortion done by organized criminals.

The history of ransomware

The first documented Ransomware attack was perpetrated in December 1989 by an evolutionary biologist named Joseph L. Popp. Back in 1989, the internet existed but it wasn't what it is today, so the attack was executed through an infected computer disk.

Popp sent out 20,000 infected disks to attendees of the international AIDS conference. The disks were labeled "AIDS Information – Introductory Diskettes." Under the guise of being a questionnaire to help users determine their risk of contracting AIDS, the disks were secretly infected with ransomware dubbed the "AIDS Trojan" also known as the "PC Cyborg."

After 90 reboots, unsuspecting victims were met with a ransom demand for $189. Popp wanted payments to be sent to his post office box in Panama, which was eventually traced. Surprisingly, he was caught but never prosecuted.

Since then, thousands of Ransomware attacks have been perpetrated against individuals, small businesses, and even giant corporations. Although Ransomware

attacks started out rather basic, they've become complex and virtually untraceable. Unfortunately, because of the profitability, ransomware attacks are here to stay forever as it's the easiest way for the cyber criminals to make money.

How do they do it?

There are several cheap and easy attack vectors that can be used to launch a ransomware attack. Cyber attackers can put in minimal effort and get maximum payout. Three of the most common ransomware attack vectors are:

- Email phishing
- Remote desktop protocol (RDP)
- Software vulnerabilities

Email phishing

Phishing rose as the most used ransomware attack vector. Using links, attachments, or both, an email phishing attack seeks to trick users into taking some sort of action. Phishing emails containing links may appear to come from a known contact asking a user to enter credentials for a bogus purpose. Those credentials are then stolen and used to access key systems on which ransomware can be installed. Other tactics include asking the user to click on a fake attachment, after which ransomware begins automatically downloading.

Ransomware is also delivered via drive-by-download attacks on compromised or malicious websites. Some ransomware attacks have even been sent using social media messaging. Generic ransomware is rarely individually targeted, but rather a "shotgun" approach where attackers acquire lists of emails or compromised websites and blast out ransomware. Given the number of attackers out there, it will be likely that if you get hit multiple times, it will be by a different attacker. Whether or not the ransom is paid, keep in mind that attackers will always try extracting useful data from a compromised machine. Assume all sensitive data on the machine was compromised, which could include usernames & passwords for internal or web resources, payment information, email addresses of contacts, and more.

Remote Desktop Protocol (RDP)

Cheap, easy, and highly available, RDP is the second most popular attack vector by a small margin. RDP ports are often poorly secured and easily compromised. Additionally, RDP security relies heavily on proper password protocol, which can be ignored by

users. Less-skilled cyber attackers can easily infiltrate weakly protected RDPs to harvest credentials. Or, if that's too much work, they can just buy RDP credentials on the dark web, with some selling as cheaply as $20 each.

Once malicious actors attain credentials, they can bypass endpoint protection and begin wreaking havoc on enterprise systems, including wiping or encrypting data backups. For organizations to gain access to their own data or retrieve it, they must transfer ransom money to a bitcoin account or some other cryptocurrency repository

Software vulnerabilities

Software vulnerabilities come in third among common ransomware delivery methods. Unpatched software not only opens the door to malware intrusions, but lays out a welcome mat as well. In some cases, when software is not properly updated or patched, attackers can access networks without having to harvest credentials. Once in the system, they begin attacking key programs and viewing or exfiltrating sensitive data. Additionally, many types of ransomware have evolved to forms that are difficult to detect, therefore extending their dwell time for maximum destruction.

Strategies for a proactive ransomware defense

1. **Prevention is better than cure**

Preventing a ransomware attack is always preferable to cleaning up after one. Implementing and enforcing cybersecurity and data protection best practices will help protect common vulnerabilities from exploitation & keep the organizations equipped to fight against ransomware attacks. The Actions which you take for Today will make Sure You're Not Tomorrow's Headline.

2. **Security Awareness**

Employees can be your organization's biggest weakness or its first line of defense against hackers. The only difference is how well informed they are. A high-quality security awareness training program will pay for itself the moment an employee recognizes a phishing email or doesn't open a malicious email attachment.

Security awareness training teaches employees to:

- Spot phishing attacks
- Create strong passwords
- Secure their laptops and mobile devices
- Connect securely on public Wi-Fi

- Notify the right people if they spot something suspicious

For best results, security awareness training should be recurring and mandatory for new hires as well as for the leadership team and every staff member in between.

3. **Email filtering and scanning**

Successful ransomware attacks are often initiated via email. Email scanning, strong spam filtering, and email authentication protocols are the most effective methods for preventing this type of breach.

Email scans can identify common ransomware techniques, block malicious URLs, and prevent employees from opening suspicious attachments.

Although they aren't new or foolproof, and they can be a bit cumbersome to deploy, when used together, these three email authentication protocols continue to be a robust defense against email initiated ransomware attacks:

- Sender Policy Framework (SPF): Restricts who can send emails from your domain and prevents domain spoofing
- DomainKeys Identified Mail (DKIM): Ensures that the content of your emails hasn't been compromised or tampered with
- Domain-based Message Authentication, Reporting, and Conformance (DMARC): Ties SPF and DKIM together with a consistent set of policies as well as links the sender's domain name with what is listed in the "From:" header
- Secure email gateways

Patch Management and Automatic Updates

If you don't have time to apply security patches, you don't have time to recover from a ransomware attack. Missed patches and skipped updates are two of the most common actions that leave networks wide open for attacks. Hackers know a large percentage of organizations don't stay current on patch management and updates, so they seek out known vulnerabilities in popular applications.

IT teams prioritize this highly effective security step by automating updates and immediately install security patches across all operating systems, software platforms, applications, mobile devices, and cloud locations.

4. Strict Access Management Policies

Privilege creep gives users far more access than they need, which in turn provides hackers with an easy path deeper into the network than they would have otherwise.

Strict identity and access management policies, such as the principle of least privilege, Zero Trust, and multifactor authentication give employees only the access necessary to do their jobs and require proof that they are allowed to do so.

5. Disaster recovery

Even if you follow all the best practices above to the letter, a successful ransomware attack is always possible. Proactively planning for recovery after a crisis is an essential factor in your ransomware defense strategy.

To help ensure your disaster recovery strategy will work when it needs to and that it covers all business-critical systems and functions, include these fundamental steps in the recovery plan:

- Fully document your entire infrastructure.
- Integrate virtualization into your disaster recovery strategy.
- Implement automated testing to ensure you can meet RPOs and RTOs.
- Test backups regularly to ensure systems and data are fully recoverable.

6. Backup strategies

Once the standard for secure backups, the traditional 3-2-1 approach is no longer effective against today's ransomware technology. Ransomware operators now target and encrypt backup files specifically, rendering them useless for recovery efforts.

Other ransomware strains enter the network, then wait—sometimes for weeks or months—before encrypting data and announcing their presence. In the period between infection and encryption, the ransomware code is copied into the backup, again rendering the files useless.

To ensure backups are safely sequestered, many IT teams have adopted a 3-2-1-1 strategy that incorporates an air-gapped copy of the data stored off-site and offline in addition to the three copies of data stored on two different media with one copy stored off-site or in the cloud

7. **Multi-factor Authentication (MFA):**

MFA should be made mandatory wherever possible to reduce the risk of unauthorized access.

8. **Cybersecurity insurance**

Organizations should consider cybersecurity insurance to help mitigate the impact of a ransomware incident. Cybersecurity insurance can be beneficial for the organizations which are often responsible for protecting customer data and have strong regulatory requirements for Cyber Security & data privacy. Some insurance companies lean toward readily paying ransoms, while others prefer to explore other remediation options, so companies should talk to prospective insurers and discuss policies before committing to an insurance provider.

Incident response to a ransomware attack

1. **How will you fight back?**

In the event of a ransomware attack, an effective response plan can mean the difference between panic and decisive action. It can mean the difference between a company-wide infection and a contained incident; the difference between swift remediation and permanent business closure. It's very important that exactly how businesses should respond to a ransomware attack and explore preventative measures that can help reduce the risk of infection.

If preventative measures fail, organizations should take the following steps immediately after identifying a ransomware infection.

2. **Isolate affected systems**

Isolation should be considered top priority. The vast majority of ransomware will scan the target network, encrypt files stored on network shares and try to propagate laterally to other systems. To contain the infection and prevent the ransomware from spreading, infected systems must be removed from the network as soon as possible.

3. **Secure backups**

While backups play a crucial role in remediation, it's important to remember that they are not immune to ransomware. To thwart recovery efforts, many modern ransomware strains will specifically target a company's backups and try to encrypt, override or delete them.

In the event of a ransomware incident, organizations must secure their backups by disconnecting backup storage from the network or locking down access to backup systems until the infection is resolved

4. **Disable maintenance tasks**

Organizations should immediately disable automated maintenance tasks such as temporary file removal and log rotation on affected systems, as these tasks can interfere with files that may be useful for investigators and forensics teams.

For example, file logs may contain valuable clues regarding the initial point of infection, while some poorly programmed ransomware variants may store important information (such as encryption keys) inside temporary files.

5. **Create backups of the infected systems:**

Organizations should create backups or images of the infected systems after isolating them from the network.

6. **Prevent data loss**

Some ransomware decryptors contain bugs that can damage data. For instance, the decryptor of a prolific ransomware family known as Ryuk was known to truncate files, effectively cutting off one byte of each file during the decryption process. While this didn't cause major issues for some file formats, other file types – like virtual hard disk files formats such as VHD/VHDX as well as a lot of Oracle and MySQL database files – store important information in the last byte and were at risk of being corrupted after decryption.

Having a backup of infected systems ensures data integrity. If something goes wrong during the decryption process, victims can roll back their systems and try to repeat the decryption, or contact a ransomware recovery specialist for a reliable, custom-built decryption solution.

7. **Free decryption may be possible in the future**

If the encrypted data is not critical to an organization's operations and does not need to be urgently recovered, it should be backed up and stored securely as there's a chance that it may be able to be decrypted in the future.

There have been instances of law enforcement agencies apprehending ransomware authors and C&C servers being found, which resulted in the release of decryption keys and allowed victims to recover their data for free. In addition, a number of ransomware groups – including Shade, TeslaCrypt and CrySis, among others – have willingly released decryption keys after shutting down their operations.

8. Quarantine the malware

Victims should never outright remove, delete, reformat or reimage infected systems unless specifically instructed to by a ransomware recovery specialist. Instead, the malware should be quarantined, which allows investigators to analyze the infection and identify the exact strain of ransomware responsible for encrypting files. Removing the entire infection makes it extremely difficult for recovery teams to find the specific ransomware sample involved in the attack.

If the malware is still running, memory dumps should be made prior to quarantine to create a full record of any malicious processes that are running. The memory dump may contain the key material that was used to encrypt the files, which can potentially be extracted and used to help victims decrypt files without paying the ransom.

9. Identify and investigate

Identifying the source of the infection is crucial for understanding how attackers gained access to the system, what other actions they took while they were on the network and the extent of the infection. Detecting the source of the infection is useful for not only resolving the current incident, but can also help organizations address vulnerabilities and reduce the risk of future compromise.

It can be challenging to identify the original point of compromise because, in many cases, the threat actors will have been on the system for weeks or even months before deploying the ransomware payload. Companies that lack the resources or expertise to perform thorough digital forensics should consider enlisting the services of a professional forensics company.

Organizations can use many free services such as Emsisoft's online ransomware identification tool or ID Ransomware to determine which strain of ransomware they have been impacted by or even virustotal.com. These tools allow users to upload a ransom note, a sample encrypted file and the attacker's contact information, and analyze the data to identify which ransomware strain has impacted the user's files. It also directs the user to a free decryption tool if one is available.

10. Decide whether to pay the ransom

If backups are damaged and there is no free decryption tool available, organizations may be tempted to pay the ransom in order to recover their files.

While paying the ransom can help reduce disruption and may be cheaper than the overall cost of downtime, it is not a decision that should be taken lightly. Organizations should only consider paying the ransom if all other options have been exhausted and the loss of data will likely result in the company going out of business. Determining the factors of when or when not to pay should be discussed and agreed prior in practice incident response exercises.

New edge solutions to protect against Ransomeware at early stage

The secret weapon AI/ML (Artificial intelligence, machine learning) wields is the power of prediction. This power is super-charged with access to more – and more refined – data points from which it can learn. Think of it like playing chess with the same partner over and over, and then doing the same with hundreds of other players. Over time you learn your opponents' tendencies and can anticipate their next move. By drawing on the lessons learned from other opponents, you have more options to consider so you can adjust your own strategy accordingly.

In the case of machine learning and data protection, stack trace analysis is the foundation of the AI/ML process. Consider this: as a program runs, there's a track record for what happens at different points in time. By analyzing what happens at each stage, normal activity becomes clear and a reference model is created. In the case of a ransomware attack, new code would be injected into this process – which is readily noticeable.

The strongest software solutions use ML that considers only the most popular reference points and excludes aberrations. This approach further refines the machine's knowledge of good versus malicious code – not only increasing accuracy, but boosting software performance, as the machine learning model consumes much less data to run.

With an ever-evolving threat like ransomware, it's not enough to have traditional anti-virus software in place, which solely defends against known threats. Active protection must be integrated with your endpoint protection to effectively defend against evolving strains of malware, also known as zero-day threats.

The value in self-protection technology and defending your systems "borders" There's a reason walls were built in ancient times: to keep the unknown out and ensure the gatekeeper's advantage. In times of cyberwarfare, walls need to be constructed around IT infrastructure & these walls could be next generation AI/ML based solutions which

can detect abnormal behaviors of your IT ecosystem and detect and protect your organization against such threats.

Today with such AI/ML based solutions; you can retain control of your data and keep danger at bay from servers to endpoints by actively protecting your borders (i.e. endpoints). With the help of AI/ML-enabled software, self-protection is possible again.

Gen-x solutions to help you protect against Ransomeware by:

- Constant monitoring for malicious activity
- Active detection for never-before seen ransomware strains
- Immediate blocking of questionable behavior
- Automatic recovery of damaged files

While the threat of ransomware is ever-evolving, Artificial intelligence - Machine learning based technologies is too. The organization should carefully evaluate & invest in such technologies to deliver advanced protection against ransomware on all fronts.

Ransomware Playbook

Ideally organizations want to avoid becoming the victim of ransomware attacks, and there are a number of steps that can be taken to reduce the risk and make the job harder for attackers. These measures take time to implement though, and while they should make an organization harder to compromise and more able to recover from attack, no organization can be completely invulnerable. As such, it is critical to have a comprehensive incident response plan in the form of playbook at place so that if the worst does happen, you are able to react quickly and efficiently to weather the storm.

It may seem counterintuitive to work on response before the incident, and even before deploying preventative measures, but we strongly recommend you do just that — develop and practice your incident response plan now. You need this in place while you work on your preventative measures so you will be prepared if you have an incident before you can fully implement your defenses. Without the proper preparation, an attack can bring your business to a grinding halt and put your critical information at risk.

A comprehensive incident response Program/Ransomeware Play book will incorporate the following:

- **Preparation -** Are you ready if a ransomware attack happens? Do you have a playbook? Does your team know what to do and who is responsible?
- **Identification -** What are your measures to identify ransomware before machines are encrypted and a message asks you to pay? How can you identify that an attack is taking place before ransomware is executed?
- **Containment -** Do you have proper methods (or have automation workflows) in place to contain threats early in the attack chain? The earlier you're able to contain the threat, the more likely you are to restrict the ability of an attacker to execute the ransomware.
- **Eradication -** Can you eradicate the threat on your own, or do you have an Incident Response retainer set up in the event of a breach? Cleaning things up is one of the last things to do in a ransomware attack. Are you able to scope the incident thoroughly to understand what happened and prevent it from happening again? Do you have the expertise on staff to eradicate the threat completely, ensuring you're not going to get encrypted in a week?
- **Recovery -** Do you have proper measures in place to recover from an attack and get things back to normal as soon as possible?
- **Review Lessons Learned -** What is your postmortem process? How can you use this as a lesson to improve your security posture?

Conclusion

A proactive approach to ransomware prevention can help organizations significantly reduce the risk of infection. In the event of ransomware incident, organizations must have effective response procedures in place to contain the incident, prevent data loss and safely initiate the recovery process.

The practices described in this whitepaper can help businesses to understand the impact of a ransomware attack, best practices to fight against ransomware. Do note, however, that these practices should be considered general and non-comprehensive advice. Security requirements can vary significantly and security systems should always be tailored according to industry, regulatory requirements and the company's unique security needs.

Section 2 - The shift to cyber resilience

Author: Nicki Doble

Cyber resilient businesses have come to accept that they will inevitably experience a potentially catastrophic cyber event, such as a ransomware attack. Mature businesses acknowledge that an attack may be successful, regardless of how well-prepared they are. Along with enabling robust and resilient defense mechanisms, they regularly practice the most effective ways to respond to such attacks. There is also a growing demand from regulators and cyber insurers to not only to prevent but to extensively plan how to respond and recover to an external cyber born attack.

Cyber aware C-suite executives are also moving away from the idea that they need to be specifically targeted, and there is now growing awareness that numerous businesses have fallen victim not because themselves were targets but cyber criminals were targeting a vulnerability and their company may be one of thousands that fall victim.

The shift in mindset from defense to resilience has a consequential affect on budgets and a business's operational focus. These two factors in turn allow a business to drive engagement across all C-suite functions.

In the past, organisations planned their BCP around constricted scenarios, where critical staff were offline for a few hours and the risk of a cyber event was apparent, but not necessarily inevitable. We now know that organisations need to view cyber security through a wider lens, and plan for scenarios where sizeable chunks of their back end and front-end operations may be unavailable for long periods of time. Unlike incidents such as a fire or theft, cyber incidents, system outages are not restricted to a location. When a business considers how it will operate if it is offline for a set number of hours, days or weeks, this forces management to involve multiple aspects of a commercial operation – particularly throughout the supply chain – which has the added bonus of broadening the base of responsibility during a security incident.

Maintaining business resilience and ensuring that C-suite staff regularly practice security response scenarios are a key indicator of how much importance a company attaches to securing their data and systems from external intrusion or internal compromise. Companies with a lax security culture tend to view security as purely a technological consideration and are likely to blame their CISO or CIO for a security event, regardless of the underlying reasons for the intrusion (attack vectors, human error etc.).

Preparation is key

Security should not solely focus on defense & prevention – time, effort and budget space should be allocated towards an effective incident response. Executives in secure organizations understand the value of a cross-functional approach to cybersecurity

Progressive management teams recognize that effective crisis planning involves multiple operational processes and diverse skill sets, and that all business functions must work together in unison, if an incident is to be contained.

Companies that do not maintain a crisis response plan are more likely to pay a ransomware demand, usually resulting from poor preparation and a sluggish response to the initial intrusion that confounds any recovery attempts. Quite often, payments are made to accelerate recovery time, limit losses and leverage insurance coverage or tax deductions to mitigate any financial damage.

Executive teams that focus on crisis management and who consider a broad range of attack vectors fare significantly better in the aftermath of an attack. Such organisations are able to engage in proactive messaging, effectively manage supply interruptions and quickly put into place manual workarounds to protect their data and maintain communication with their customer base. Robust cybersecurity protocols allow a business to act in a way that addresses any threat of legal or regulatory action and minimise the overall cost of the attack, including any residual reputational damage.

Planning tips

- Companies that undertake effective planning are better equipped to manage an incident by nominating a point person that co-ordinates a response and reports to Board. Inexperienced organisations tend to have their CEO or CIO or manage the indent, which often means wearing multiple corporate hats, which sometimes makes objective decision making a lot more difficult than it should be.

- Blame culture often leads organisations to point fingers unnecessarily when things go wrong. Executive teams should agree in advance on a set of decision principles that management works within the event of a crisis. A company's security culture should recognise that not all decisions will be correct, and hindsight applied in a Post Incident Review (PIR) will always have the benefit of knowing the outcome of a set of actions. Therefore, having constructive decision principles helps individuals make the right decisions at any given time, even if in hindsight that decision turns out to be the incorrect.

Cyber insurance is only part of the solution

Cyber insurance should form part of your holistic cyber security strategy, it is one piece of a larger puzzle. It does not prevent an attack, and it won't cover all your losses. Some policies require you to use an insurers choice of incident response provider. Whilst this shouldn't present too much of a problem, it does mean that your organization may not be in full control of an incident.

Insurers are also starting to provide additional technical services, such as threat intelligence, vulnerability updates and table top scenario kits. All of these are welcome benefits but are essentially loss mitigation tools. Insurers know that if you keep your systems up to date and prepare for an event, the financial impact is greatly reduced.

Cyber insurance is increasingly viewed as a must-have add-on to corporate cybersecurity strategies, but as the costs of insurance payouts continue to rise, insurers will continue to look at who they cover, and how they offer assistance. What happens in a scenario where your organization was provided guidance, but you failed to act? Insurers won't cover your car if you drink drive, you have bald tires or your vehicle is unregistered – will they need to apply the same principles if your organization make a conscious decision not to meet a minimal standard?

The role of the C-suite in a successful cybersecurity operation

Cyber security requires collective ownership and the c-suite need to pull together to create resiliency. Businesses leaders solve complex problems all the time and the c-suite should not see cyber security as different and should work cohesively to mitigate cyber risk.

Moving the conversation from a cyber-attack may happen to it will happen, helps leaders map out how they will respond, their areas of accountability and how as a leadership team they plan to lead and present to their employees, the board and the market.

CEO – Chief Executive Officer

Chief Executives are accountable for the overall performance of a company. With that in mind, considering the billions of dollars that cybercrime has cost companies around the world, not to mention its potential for reputational damage, cybersecurity should not be the sole property of IT teams.

Reports of cyber attacks are on the rise, and customers are more concerned now than ever before about the security of their personal information. Accordingly, whilst outdated thinking about security being a technology problem still exists amongst C-suite executives, the general public strongly disagrees. Public opinion is a key factor in a CEO keeping their job following a security breach. CEOs are much more likely to resign or be fired when the public believes the company was not adequality prepared or failed to protect their information.

CEOs should be preoccupied with creating a robust security culture and invest their time and resources towards promoting said culture at any opportunity. Following a cybersecurity event, C-suite management skills are closely reviewed. A leader's calmness and composure makes a significant difference to how teams respond during an incident, and how well a company is perceived throughout said incident. Executives that are prepared and require their staff to undergo regular practice scenarios are more likely to be perceived as a steady pair of hands, both in the eyes of the Board and the general public.

CFO – Chief Financial Officer

CFOs don't necessarily have to understand the technical minutiae of cybersecurity planning, but they must be aware of the financial risks associated with an ever-increasing threat of intrusion. Given that any data breach could seriously impact the reputation of an organisation, damage cashflow or incur significant fines (eg. GDPR), the CFO needs to have a clear understanding of how much a successful attack could end up costing a company – both in the short and long term. Whilst a CISO can offer guidance on attack vectors and technology, a CFO can improve cyber resilience by assisting in translating risk into a language better understood by senior leadership – usually by relating it to budgets, finance and expenditure - and ensuring adequate financial consideration is given towards preventing an attack and mitigating risk.

The CFO should also be involved with the legal and technical team when determining cyber insurance coverage. The decision to mitigate or to transfer strategic risk needs is a conversation that extends beyond IT. Based on the decisions as to what risk will be accepted, the CFO needs to plan for how the organization will cover any financial gaps between the actual financial loss and the reimbursement of insurance, particularly if there has been reputational or IP loss that may impact future revenue targets or increase marketing spend.

COO – Chief Operating Officer

The COO focuses on ensuring that all parts of a business are working together to achieve the same set of goals – not only by protecting the business from internal threats, but by improving the supply chain operation's cyber resilience and making it more

The COO has the ability to influence change throughout the organisation and move away from traditional, reactive attitudes towards cybersecurity, and embed progressive security principles throughout the entire operation. Like the IT concept of "Security by Design" the COO can change an organizations way of working by making constant incremental changes to build in secure and resilient operations rather than a costly and reactive recovery transformation.

CMO – Chief Marketing Officer

Building digital trust with a customer base is fast becoming a strategic pillar for showing people how considerate a company is towards the data entrusted to it by the general public.

Brand and reputational damage can be difficult, if not impossible, to wholly overcome (at least in the short term). Building a robust cyber security operation - coupled with ease of user experience - can and should become an important marketing tool in its own right. Customers may not always be consciously aware about their data, and being able to assure them that a site or platform is safe and secure can be a valuable asset towards attracting and retaining customers

CMO's should also consider how the company should respond if criminals manage to spoof their email domain and send phishing communication to their customer base. How will your band respond to ensure your customers know malicious actors are hijacking your brand? Have you already built in safeguarding protocols, or will you need to rush out a fix to protect your customers and your reputation?

Chief HR Officer (CHRO)

The role of HR in a cybersecurity operation is multi-layered and considers people, data, cyber talent pipeline and post event reviews to varying degrees

People, rather than IT systems, are often the weakest link in the chain. A company's HR team plays an enormous role in launching creative programs to cultivate a 'security first' corporate culture, starting with a security conscious onboarding procedure.

There is a global shortage of well-trained cybersecurity staff, and the best security teams have people with diverse skill sets. Internal training programs can help build a pipeline of talent whilst increasing overall awareness.

HR teams are the owners of employee and applicant data, with a big responsibility in ensuring data remains secure at any given time.

Here are some questions to reflect on:

1. Are your teams collecting the right information, do they understand the importance of data minimsation?
2. Are they ensuing they conform to data retention policies?
3. If a cyber attack takes payroll offline, do they have a plan that ensures the company can keep paying its staff members?
4. Do they have an investigation framework ready that enables them to objectively asses at how events unfolded across the entire business?
5. If the event was due to an employee fault, are they confident the company is able to avoid wrongful dismissal payouts, if the employees had concerns and risks that were not listened to or adopted by the business prior to the event?

Chief Legal Council

General Councils need to determine if the company may face litigation from a cyber incident. Cyber security is now commonly written into commercial agreements, is the company liable for a significant a contract penalty or instant termination of contract in a cyber event? In some countries data breeches are becoming very litigious, do team members know what they should and shouldn't say in the heat of an incident response on corporate channels?

Legal councils also need to be able to quickly ascertain the law and regulations in the different states and countries that the company operates in. Practicing scenarios ahead of time allows legal and media teams to know and respond to required timelines with the correct information to the write parties during an event.

They should also be involved in the cyber insurance negotiations.

C-suite collaboration

C-suite executives are sometimes reluctant to share their organizations' cybersecurity incident information externally – and understandably so, in some cases, although this doesn't make any cover-ups in any way excusable. Given that the CHRO, the CMO and the CFO possess stewardship for the most coveted data sought out by hackers, they should be sharing ideas and learning from their peers within their sector.

A reluctance to share information is largely driven by a lack of cybersecurity knowledge, or not wanting to share company info with competitors. CISO's can help their colleagues to learn from their peers by providing them a range of topics they can discuss. HR, Finance and Marketing vendors can also play a role in bringing together clients to discuss how the company protects their data, rather than events based purely on siloed business functions.

Cyber criminals are known to collaborate and share information. In order to stay one step ahead of them, C-Suite executives need to be prepared to do the same.

The cost of cybersecurity

C-suite executives should approach cyber security as a strategic function that will ultimately bring value to their product offerings beyond risk mitigation, in the form of competitor differentiation and digital trust (see above). They should also move away from the idea that cybersecurity is necessary evil on corporate budget sheets. Such thinking leads to inadequate technological solutions and lax security practices.

That being said, a cybersecurity operation should not become a money pit. Firms that are lagging behind should consider a one-off transformational investment to implement controls and affect cultural change across their entire organisation. Once a transformational spend is complete, security budgets normalize and costs level off with less holes to plug, and the move towards a proactive security operation. Guidance on where to focus during a transition can be led by scenario practice runs, along with the associated cultural and technological changes.

Conclusion

The world of commercial IT changes at a rapid pace. Over the last 5 years or so, most of this change has occurred within the twin pillars of a company's cybersecurity operation – cyber resilience and cyber defense, and it is the former that provides companies with the most bang for their cybersecurity buck.

The days of relegating cybersecurity to a cursory mention on annual business plans are long gone. In the age of cyber resilience, attacks are *presumed*, not theorised, and a

company’s response to a major intrusion should be meticulously planned and adherent to a rigid set of goals endorsed by all members of the C-suite team.

Throwing money at state-of-the-art cyber defense mechanisms – routers, firewalls, antimalware and secure WAN networks – is the easy part. What’s more difficult is promoting a 'security first’ culture, learning how to limit the reputational and financial damage that occurs once a criminal has gained access to your data (and that of your customers), and keeping a cool head when such an incident occurs.

The overriding theme is to plan, plan and plan again. The most damaging cyberattacks have the potential to take entire companies offline for days at a time. Your organisation should leave no stone unturned in its efforts to improve cyber resilience, and it all starts at the top, with a progressive attitude towards cybersecurity emanating from C-suite employees, which in turn affects the behaviour of front-line staff.