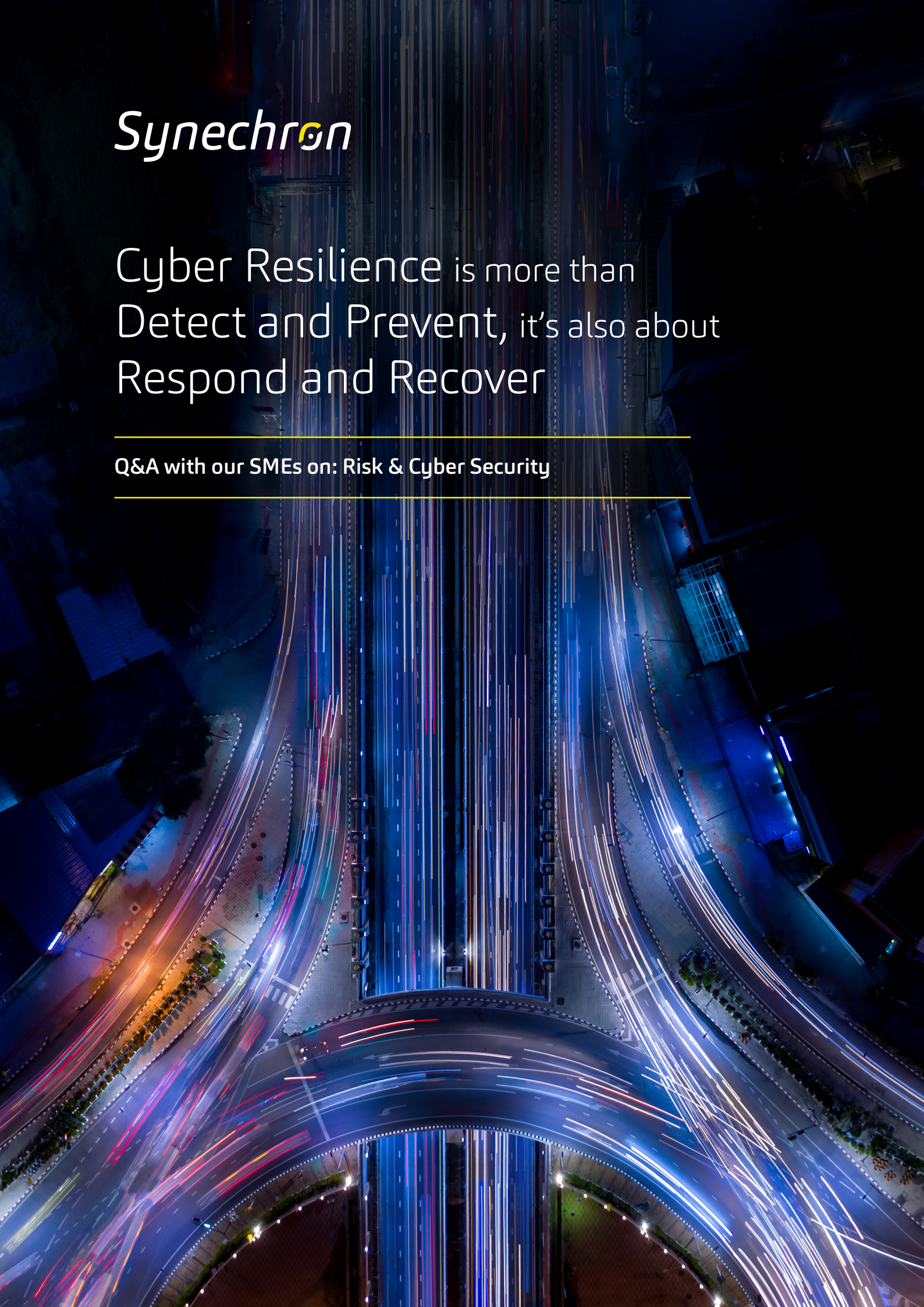


Synechron

Cyber Resilience is more than Detect and Prevent, it's also about Respond and Recover

Q&A with our SMEs on: Risk & Cyber Security

Resilience from cyber threats is more important now than ever. The year 2020 broke all records when it came to data lost in breaches and sheer numbers of cyber-attacks on companies, government, and individuals[1]

With most of the online workforce working from home and relying on personal broadband connections that are often lacking the tight security found in an enterprise environment, hackers are exploiting this vulnerability.

Phishing and spear phishing, Ransomware, Doxing, Credential Stuffing, DDoS, and insider threats abound. Could we recover from a modern cyber-attack? We speak to Synechron's and Synechron Digital's SMEs about risk and cyber security to find out how enterprises have evolved their strategies to outthink criminal minds.

Gavin Wilson

Principal Consultant
London, UK

Enterprises have focused for some time on controls to identify, detect and protect/prevent cyber threats. But are organizations adequately considering how to respond and recover if an attack was to occur?

Most organizations have developed some form of incident response capabilities. Yet, those capabilities are often focused on short-term responses and are usually classified and considered as an IT issue only. This type of approach may fail to address the wider impacts of a major cyber incident and may result in turning an incident into a crisis for the organization.

A response and recovery approach is critical to avoid and/or mitigate a cyber crisis which often comes down to how an organization properly manages a cyber incident before, during, and after the occurrence. An organization cannot expect to just be able to respond to a cyber incident if unprepared. The organization's readiness prior to an incident occurring is essential. Readiness equates not only to vigilance, for example in the form of ensuring 24/7 monitoring tools and alerting, it also requires clear and concise processes and procedures detailing how to respond, as well as trained resources to execute the response. A well-prepared, multifunctional team must be poised to deal with all aspects of an incident at any time, not only from a technical response and recovery perspective but in addition to business continuity and stakeholder communications, especially if the organization has experienced a breach of sensitive user data. Crisis simulation/service outage rehearsals enable management to understand the type of scenarios that can occur, what steps to take, and whether the organization is truly prepared to deal with a major cyber incident.

How seriously organizations take a cyber incident preparation starts with executives taking a broad view of cyber crisis management and setting the tone which cascades down the organization. Executives can often see cyber incidents as only "an IT issue". However, management teams need to recognize that effective crisis planning involves multiple functions and skill sets and needs to ensure support and sponsorship is given to the organization to implement cross-function preparation and training. That ensures a highly coordinated response and recovery if an incident is to be contained, or to ensure an incident does not escalate to a crisis level.

Response management to a major cyber incident will often kick-off via the uncovering of a security breach, which is often caused via hacking or even negligent employees. The objective of a coordinated response to the cyber incident is to limit the loss of time, money, data, and customers, as well as to control the damage to reputation and the costs of recovery. The key steps are for the response team to gather the required resources and to find the cause and impact of the breach so mitigating steps can be taken, potentially to isolate an affected system to reduce a wider organizational impact. Whether you handle as an organization, you handle your IT within the company, or you outsource it, it is important to notify the department about the breach. Management must then be prepared to communicate, as needed, across all media including social media, in ways that assure stakeholders that the organization's response is equal to the situation.

Dependent on the exact nature of the cyber threat It's important to notify your employees and/or your customers of the breach. Problems such as these are best presented upfront and honestly. Keep everyone up to date and inform them of the steps being taken by the organization and the IT team to resolve the issue.

Recovery steps to return to normal operations and limit damage to the organization and its stakeholders will continue after the incident. This will include assessments of the root causes and of the management of the incident, and to ensure any remediation actions are implemented to mitigate a reoccurrence of the incident. Wider recovery, depending on the extent of the cyber-attack, will depend on an organization's recovery time objective to return systems and business to normal. Quicker recovery times require investment and executive support.

Good response and recovery management is not about preparing for one specific event. It's about the creation and implementation of broad, flexible capabilities that enables a targeted response to a wide range of scenarios. Digital assets now drive a huge portion of an organization's value. Senior executive teams can see and read for themselves the increased cyber threats of today, and they need to focus on preparing highly effective cyber incident response and recovery capabilities.

How are cyber threats different now to, say, two or three years ago?

The risk and severity of cyber-attacks has grown over the past few years. Since 2018, organizations have seen more cases of cyber-crimes related to massive data breaches, ransomware, account hijacking and many more.

The advancement of technology, and the wide use of digital media, is allowing attackers to take advantage of individuals and firms who make cyber security a lesser priority. They will target everything from a newly-launched social media site to an established online system in order to gain access to sensitive information.

Every other day we read news related to cyber security threats, like ransomware and phishing. Plenty of us have received emails, appearing to be from HMRC or the Royal Mail, etc. which can appear very convincing, especially to non-tech savvy individuals and even tech professionals can be fooled.

The increased level of cyber security threats has changed over the last two to three years. It continues to evolve, especially in industry and societal technology growth areas which have seen an increase in the usage of Cloud, growth in social media usage across multiple platforms, and the advancement of Artificial Intelligence (AI). The cyber threat in these areas is matching the growth in popularity as organizations continue to move services to the Cloud, social media sites are increasing their users bases, and with advancements in AI solutions for businesses. These areas have affected the growth in different attack vectors for cyber criminals over the last couple of years, specifically exploiting Cloud vulnerabilities, social engineering attacks and AI-enhanced cyber threats.

Here are three areas of greatest vulnerability:

Cloud Vulnerability - Cloud vulnerability is, and will continue to be, one of the biggest cybersecurity challenges faced by organizations. The continued cost benefits and convenience for organizations to utilize services in the Cloud means more business decision makers will engage in a Cloud strategy, and reduce the on-premise technical infrastructure. As a result, more sensitive data related to employees and business operations will be stored on the Cloud

The adoption of the Cloud has created challenges for firms given the ever-increasing percentage of the enterprise workload that are now on the cloud. These organizations make tempting targets for malicious hackers who target organization systems causing data breaches, misconfigurations, account hijackings and DDoS attacks which are among the top Cloud security threats.

A key consideration for an organization moving to the Cloud is ensuring investment in a robust Cloud security strategy. This includes ensuring Cloud service providers meet industrial security standards and continue to improve and evolve Cloud security in line with the advancements of cyber-attacks.

Cloud companies like Google and Amazon who store other companies' data are heavily investing in improving their Cloud security, and providing suitable options for organizations wanting to gain the benefits from moving to the Cloud. However, that doesn't make them immune to deep cyber intrusions.

Social Engineering Attacks - Today, social media is regarded as one of the biggest security risks to organizations and individuals, with many high-profile organizations blocking social media from corporate networks to reduce the risk of cyber breaches. One technique social engineering attackers rely on is the attackers tricking the victim into carrying out actions that result in the organization or individual giving up sensitive information, such as account names, passwords, bank details, etc.

Social engineering attacks have increased over the last couple of years, in line with the popularity and continued increased use of social media, email marketing, blogs, etc., which are used on various platforms by many age groups. The main social engineering threats are often non-technical and do require the direct hacking of devices or systems. This provides different challenges to organizations and their executives.

It is normal for attackers to focus on individuals' inherent helpfulness or to try to manipulate a person's concerns or worries. For example, an attacker can call or email and feign an urgent issue that demands immediate network access. The most popular form of attack over the last view years is phishing, whereby attackers trick victims into surrendering sensitive information, like debit card details or bank account information. This is often done through a false email from a well-known brand. Given the wide population, phishing is a low-cost and effective way for attackers to gain sensitive information and will continue to be a serious threat.

The growth of social engineering attacks will continue as the success of an attacker is dependent on an individual recognizing the threat. Although there are technical mechanisms to help thwart social engineering attacks, the best

protection against such is ultimately being able to train and provide an employee base that is able to identify and react appropriately to typical social engineering threats/attacks. Awareness is the first key step to stopping individuals from executing social engineering attacks. This goes hand-in-hand with continued organization-wide education and internal penetration testing to review the effectiveness of internal training.

AI-enhanced Cyber Threats - These are a form of cyber attack expected to grow in the future with the advancement of Artificial Intelligence in many industries. AI is gradually finding its way into businesses and into cyber security. Intrusion detection systems enabled on organizational networks can be set to look for data patterns, spurious traffic, and act accordingly if suspicious activity is detected.

However, as this type of technology increases in industries, where AI can help enterprises detect and fix vulnerabilities in their systems, these same AI capabilities are being used by hackers to launch sophisticated cyber-attacks utilizing complex adaptive malicious software. These types of attacks have grown and advanced over recent years, and it's likely these types of attacks will be one of the big types of cyber security threats in the future.

To what extent has the pandemic changed the cyber threat landscape?

The COVID-19 pandemic has resulted in a shift for many service organizations to adopt a strategy allowing the bulk of their workforce to move to remote working. Although remote working in organizations was not a new concept before the pandemic, where an employee may have occasionally worked from home, the sudden shift in the entire office/IT workforces completely working remotely for a prolonged and sustained period came as a sudden requirement to most IT departments who had to facilitate the capability rather rapidly.

The necessity to facilitate mass remote working with a higher usage of Virtual Private Networks (VPNs) and End User Devices (either company laptops or Bring Your Own Devices – BYODs) often via a home Wi-Fi, has changed the cyber threat landscape for organizations.

Virtual Private Networks - With many employees working from home, enterprise virtual private network (VPN) servers have now become a lifeline to organizations. Their security and availability are a major focus to ensure individuals can access the required work resources to perform their day-to-day tasks. A threat to organizations is ensuring these VPNs are configured correctly, and are secure and resilient against cyber-attacks to reduce the risks of exposing sensitive information on the internet.

End User Computing- As more employees have company laptops or are working using BYODs, which are unlikely encrypted and are relying on a home Wi-Fi, this can mean less protection of a corporate network. Working from home or, in some cases working from anywhere on open public networks, does not guarantee the same level of cyber security as an office environment would. Personal laptops, tablets, and phones outside of the corporate network are more exposed. For example, antivirus or anti-malware scans may not be completed as regularly. Individuals can use these devices to access websites from home via their public internet service provider, whereas in an office environment internet browsing policies would have denied the user access to certain websites. These websites may contain malicious software, etc. which may then be downloaded onto the user's device.

With this increase in individuals working remotely comes an increased risk of being exposed to cyber-attacks, such as phishing or malware. This can be perilous if unknown attachments are opened or certain links are opened to malicious websites. Although these types of attackers certainly existed before the pandemic, the world has seen a huge increase in COVID-19-focused cyber-attacks. Attackers are using the COVID-19 environment as bait to impersonate brands and to mislead employees and customers. Over the last year alone, tens of thousands of fake websites have been set-up related to COVID-19 -- from offering items such as face masks and hand sanitizers to simply offering tips or eBooks on how to stay safe during the pandemic. Since the start of the pandemic in 2020, there has been a single global theme for attackers to exploit—those who are taking advantage of people's fears and insecurities related to COVID-19.

Graham
Fletcher

Associate Partner
Greenwich, UK

Disaster Recovery testing and Business Continuity planning has traditionally focused on large events that could cause partial or total failure of a Datacenter. Is this sufficient planning and testing for the new threats?

The short answer to this question is, "necessary but nowhere near sufficient." Physical threats have not gone away. If anything, climate changes make threats such as fire, flood and disruption to essential services even more likely, so business continuity planning and resilient architectures to mitigate the effect of these types of physical threat are more crucial than ever. It should also be recognized that high availability architectures have evolved over the years so that Disaster Recovery (DR) is less about recovery to a secondary DR site over a period of several hours but increasingly as a warm secondary site where data is replicated, or even where both sites are active simultaneously and either can take the full load if needed.

While these improvements have huge benefits to the speed of recovery (recovery time) and the granularity of data recovery (recovery point), they are reliant on rapid synchronization of data between the sites, and this can be a disadvantage when considering some of the new threats.

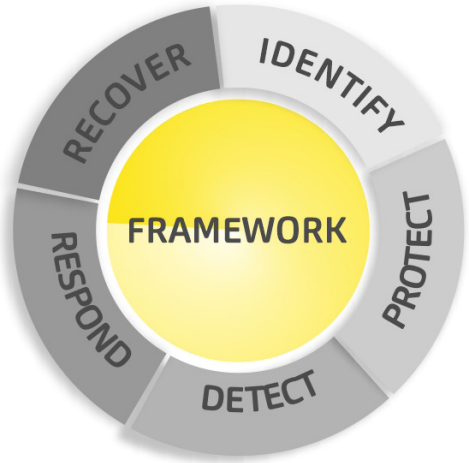
The NotPetya malware attack targeting Ukraine in 2017, used the Shadow Brokers' Eternal Blue as well as mimikatz exploits to rapidly propagate within corporate networks. Some companies lost all of their Windows infrastructure in a matter of hours and, in some cases, backups were also compromised as a result of the severity of the attack. The very mechanisms that allow rapid recovery from more traditional threats, just give the malware an additional lift as it is replicated and destroys the very infrastructure you may rely on for recovery.

As if that is not bad enough, just to add some additional spice to the problem, malware can also be dormant. Dormant malware may lie undetected and benign in an organization for some time before being triggered by some event or a predetermined time. So now the time and duration of infection need to be considered, as well as the point in time that the malware's payload is triggered. This is a tricky aspect to consider when deciding how to recover infected machines. Although we are likely thinking of a very obvious and visible threat, such as encrypting ransomware when we consider these threats, there are many other more covert threats that can sit undetected in an environment allowing command and control channels for attackers, for example.

Protection of backups, planning and testing for response and recovery from sophisticated cyber-attacks, is essential but not easy. Backup to tape provides a natural "air-gap" so it provides some protection. But many organizations scrapped tape backups some time ago in favor of on-line backups. Even when they exist, typically tape backups are only taken once a day and will likely not come close to meeting business expectations for recovery. In addition to existing backup solutions, additional cyber-resilient backup strategies and solutions are increasingly being considered. Threats that encrypt data and compromise core dial-tone infrastructure may mean that recovery from bare metal is needed. Understanding the dependencies in advance, the impact to recovery times and impact to data integrity, is essential. Likewise, rehearsal of a major recovery like that is essential to ensure that assumptions and dependencies are correct, and that collective muscle memory is fresh and current when needed.

How should a risk and control framework be adapted to cater for the new threats?

It is tempting, and likely correct, to prioritize the 'Detect and Prevent' controls in risk and control frameworks based on the assumption that prevention is always better than a cure. Even though this approach may reduce the probability, and sometimes impact of a serious incident occurring, neglecting to adequately consider 'Response and Recovery' can leave an organization with serious exposures should prevent and/or detect controls fail or are bypassed. Even if we can reduce the probability dimension of residual risk to very small, for some of these new scenarios impact can remain very high.



NIST Cyber Security Framework

An instructive exercise can be to use scenarios to test a control landscape through the lens of a scenario with a high-impact attack vector. So, if we take Ransomware for example and examine the whole control environment across, say the NIST Cyber Security Framework of Identify -> Protect -> Detect -> Respond -> Recover, we can see where the controls are concentrated and where we may need to augment our control environment. We can ask questions like: "If our 'Detect and Prevent' controls fail or are bypassed, do we have robust controls to 'Respond and Recover'?" or "Are our backups sufficiently protected?", "Do our High Availability architectures consider the impact of ransomware?"

What training activities might be appropriate to prepare for a cyber response?

Testing recovery from cyber scenarios is hard. Traditional 'Disaster Recovery' testing for a full or partial datacentre failure is hard enough, and many organizations still struggle to do realistic full-scale testing where networks are isolated, for example. A safe but realistic test, of say a ransomware attack, is very difficult to achieve in practice. Training and classroom-based scenario planning therefore become essential tools for driving out missing steps in recovery runbooks and developing muscle memory. The time spent developing detailed, rich and relevant scenarios is time well spent as these scenarios can be used for other things as well as testing and training, and bring to life concepts that can seem quite theoretical, abstract or unrealistic otherwise.

Considering scenarios in itself can take some effort as, in order for this to be effective, teams should aim to consider scenarios that have not previously been considered and include low probability/high impact scenarios as well as more likely low impact scenarios. Testing, training and rehearsal of recovery runbooks for low probability/high impact scenarios is particularly important. However, this may be the only opportunity to be sure that an organization is ready to respond to those kinds of attacks.

Collaborative scenario planning and tabletop exercises are both foundational training activities that are relatively low-cost and, at the same time, allow engagement of multi-disciplinary teams in an environment that encourages challenge and creative thought. With only a modest investment in the training environment and attention to detail in creating the training scenario, a very realistic atmosphere can be created. Use of frequent injections that vary the scenario during the session can help to replicate the uncertain and evolving nature of a cyber-attack and test teams' abilities to adapt to the changing circumstances.

While detailed scenarios and runbooks provide a good baseline, a really mature response is where the teams are comfortable to go off-book when needed. A real incident is unlikely to match exactly the scenario rehearsed in the classroom, so arguably the most valuable benefit comes from the inter-team working across the multi-disciplinary functions needed to respond to a threat like this. Tabletop exercises can allow teams to practice building consensus and taking decisions quickly together. Assign observers to the session to capture lessons learned and ensure that feedback can be given in such a way as to encourage learning.

Correctly delivered and facilitated, tabletop exercises allow assumptions and dependencies to be tested and also for multi-disciplinary teams to test demarcation boundaries, develop mutual credibility and trust across teams, and develop collective muscle memory in a collaborative, inter-team working manner.

Beyond the classroom, small drills and functional tests can be developed that can be used as training exercises and ultimately building up to safe variations to the scheduled Disaster Recovery test schedule to include new scenarios where possible. Ultimately, fully functional environments, so-called "cyber ranges" that can simulate real cyber-attacks, are the nirvana for training and testing these types of threats, but investment is high.

Resources:

[1] Brooks, Chuck, "Alarming Cybersecurity Stats: What You Need To Know For 2021", Forbes, 2021

[2] Greenberg, Andy, "Sandworm – A new era of Cyberwar and the hunt for the Kremlin's most dangerous hackers", Doubleday, 2019, ISBN 978-0-385-54440-5

[3] https://www.nist.gov/cyberframework

[4] https://www.techopedia.com/definition/28613/cyber-range

About our SMEs:

Gavin Wilson
Principal Consultant
London, UK

To know more about Gavin

https://uk.linkedin.com/in/gavin-wilson-53302730

Graham Fletcher
Associate Partner
Greenwich, UK

To know more about Graham

https://www.linkedin.com/in/grahamfletcher

www.synechron.com