Rebuilding from a cybersecurity breach.

modis

The threat landscape is more complex than ever.

The global cost of cybercrime will grow from $3 trillion in 2015 to $6 trillion by 2021.[1] In fact, the World Economic Forum's 2017 Global Risks Report identified the world's increasing cyber dependency leading to the risk of a massive attack as one of the top five trends.[2]

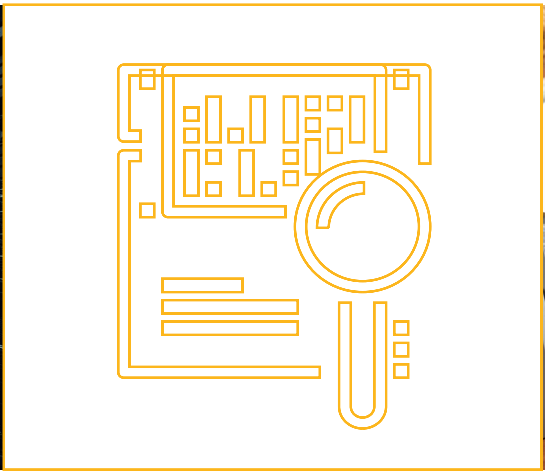
Criminals don't even need cyber expertise to launch attacks anymore: ransomware tools and ransomware-as-a-service are available to criminals, and they can be easily customized. "Businesses need to invest heavily to match the growing threat of cybercriminal activity, in each of technology, internal security personnel and training of general staff to identify and avoid threats," the analyst firm Frost & Sullivan said.[3]

In May 2017, the security news was all about WannaCry. The attack, which reportedly locked out users within an estimated 250,000 organizations in 70 countries, was especially pernicious because it combined ransomware with a worm that allowed it to spread across networks instead of infecting a single computer. Computers within Telefonica, FedEx, Deutsche Bahn and Britain's National Health Service were among those hit.

WannaCry was followed almost immediately by reports that another virus, Adylkuzz, was taking over individual computers and causing them to subvert the Bitcoin ecosystem.[4]

Next, June 2017 saw still another global attack that halted business operations in 64 countries.[5]

Cybersecurity firm eSentire predicts that the Shadow Brokers, the criminal organization that stole a vulnerability from the National Security Agency than enabled WannaCry, will be back with more stolen cyber weapons, while more criminals, inspired by the success of WannaCry and schooled by its methods, will try their hand at cracking into the world's most sensitive data.[6]



Changes in attacks and responses to legacy vulnerabilities

A connected world provides a constantly expanding attack surface. At the same time, many well-documented existing holes remain unpatched. A case in point is WannaCry, which exploited Windows XP. Even the NSA, source of the stolen cracking tools used in this ransomware attack, uses XP, which no longer receives support or security updates.

The U.S. Government Accountability Office placed the 2020 Census on its High Risk List due to its reliance on technology and the government's reliance on legacy systems.[7]

In May 2017, the White House issued a Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. However, it could take years before government systems are fully secure.[8]

The situation at an enterprise level is somewhat better but not excellent. A survey by IT professional community Spiceworks found that 14 percent of business PCs in more than half of all business organizations still run Windows XP.[9]

Connected Cars Under Attack

Passenger cars have become increasingly complex and computerized. In 2014, security researchers reported that connected cars were vulnerable via connectivity functions, their sensors and their computerized systems.[10]

Moreover, newer models can be unlocked and even remotely started using mobile phone apps — apps that can be easily hacked, cybersecurity firm Kaspersky found.[11] RSA warned that while security professionals must keep their eye on high-value targets such as infrastructure, they shouldn't ignore easier targets such as cars[12] or smartphone fingerprint readers.[13]

Threat to Hardware and Embedded Systems

Hackers have turned their attention to hardware as well as software. Scott Borg, Director of the U.S. Cyber Consequences Unit, recently told a group of hardware engineers that criminals have moved their focus from operations control systems to programmable logic controllers and embedded devices.

> **"You people are now in the crosshairs; [design] decisions you are making will have powerful security implications."**
>
> —Scott Borg, U.S. Cyber Consequences Unit

"Initially," he said, "they focused on operations control, monitoring different locations from a central site. Then they moved to process control, including programmable logic controllers and local networks. Then they migrated to embedded devices and the ability to control individual pieces of equipment. Now they are migrating to the actual sensors, the MEMS devices."

The Internet of Things remains highly vulnerable. As cities become smarter, they become more open to hostile manipulation.[14] Smart grids, connected transportation systems, traffic lights, smart street lighting and security cameras can be hacked.

Market Manipulation

Cyber criminals can make big money by manipulating the stock market. In 2015, a criminal ring stole more than 100,000 press releases before they were made public and used that information to make more than $100 million.[15]

In another case, hackers broke into the systems of financial institutions and brokerages, then used the stolen customer data to manipulate stock prices.[16]

Best practices to recover from a breach

Security experts agree that organizations should behave as though a cybersecurity breach is inevitable. In 2016, Gartner Research Director Rob McMillan warned, “Your business must be prepared — an intrusion is inevitable for many organizations and preventative security measures will eventually fail. The question you must accept isn’t whether security incidents will occur, but rather how quickly they can be identified and resolved.”[17]

A prepared organization has an Incident Response Plan ready for this situation. The plan should be crafted by a cross-functional team that includes not only IT, but also the C-suite, legal department, privacy officers (if the company has them), and the public relations or communications staff.

The incident response plan lays out the procedures for dealing with a breach and its fallout. It acts as a template for a customized approach to the individual incident.

A 2012 benchmark report by the Ponemon Institute found that organizations can greatly reduce the cost of a data breach by having an incident response plan, a strong IT security posture and a Chief Information Security Officer.[18]

These are the six steps every organization should take when a breach occurs:

1. Assess and isolate the damage.

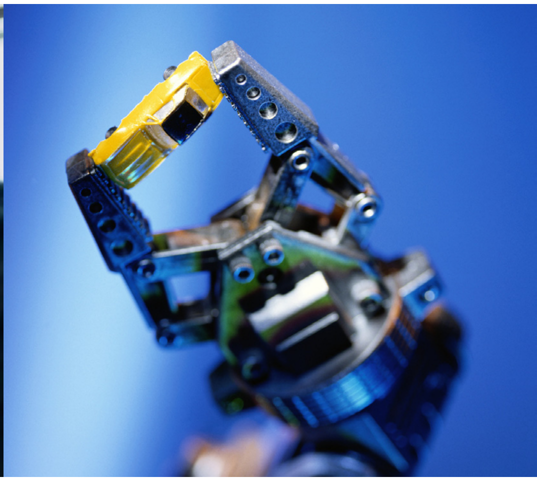
Isolate both the physical location of compromised hardware and the software or systems that were damaged. Data protection provider Digital Guardian recommends taking all affected machines offline, but leaving them running. Wait for the forensics team to begin investigation instead of letting regular IT staff examine files.[19]

It’s important to begin documenting everything about the intrusion and potential data loss or compromised systems as soon as the breach is discovered. Make read-only images of all affected machines. There should be a designated person or persons on the incident response team charged with documentation. If not, immediately draft personnel to do this.

Digital forensics may be provided by an expert internal team or an outside vendor. The team should be trained on digital forensics tools with a focus on investigating intrusions and data theft; and, in this multi-device era when many intrusions begin with the insertion of an infected thumb drive, it should be well-schooled in analyzing mobile devices and embedded devices. Computer forensics can also determine whether an employee was responsible for data theft.

Assess whether business functions were impaired, what data resides on machines or networks that were compromised, whether data was compromised or stolen, and whether digital evidence was destroyed or modified. Forensic analysis should be applied to all client devices, such as hard drives and memory, network traffic and applications. All network traffic should be captured and all packets stored for forensic analysis, according to Digital Guardian. The forensics team should evaluate archived traffic to look for anomalies or red flags. Forensics solutions automatically capture and analyze data in real time, providing immediate access to the data needed to understand the breach. If the company doesn’t use such a solution, logs and files must be manually reviewed.

Note how the breach was discovered, all personnel involved and whether any hardware is missing. As more information becomes available, continue with complete documentation. Establish a chain of custody for hardware and for data in case criminal action can be initiated.



2. Repair the network.

Certainly this is the most obvious and compelling step to take, but this work should not begin before the breach has been fully documented. Identifying the root cause of the breach not only allows the company to fully contain and heal the network, it also will inform planning for future prevention measures.

In addition to the network itself, other repairs or actions may be necessary. For example, if the intrusion came via a company-issued mobile device or application, devices may need to be upgraded or swapped out. If the intruder stole customer passwords or information, all should be notified to change their passwords. In the case of credit card data theft, new cards should be issued to all affected customers.

3. Communicate the breach.

This should be done concurrently with the first two steps, at the same time that security teams are assessing and then repairing the damage.

- Internal teams and executives should be informed immediately.
- Alert legal counsel to decide whether law enforcement should be brought in and/or customers notified.
- If customers and clients are affected, they should be notified promptly. State and federal laws mandate notification in certain cases.
- If it seems likely that the incident will be deemed newsworthy, it's better to proactively reach out to selected media.

Many companies are reluctant to admit to a breach. However, if customer data has been stolen, it's important to be transparent. While this can certainly have a negative impact, if and when the breach is finally revealed, it becomes a double negative: not only was there a breach, but the company attempted to hide it.

According to data protection provider Digital Guardian, you should use these tactics for going public with the information:

- If appropriate, admit fault. In any case, accept responsibility for securing your network and data. Promise to do everything possible to mitigate damage to those affected.
- Provide details of what happened and, if possible, how and why the breach occurred.
- Be explicit about possible solutions and mitigations for those affected by the breach. If possible, provide a special offer or services. For example, when consumer data is stolen, companies sometimes offer a free year of identity protection services. Prepare responses to common questions from those affected; designate a team to respond to concerns within hours and across communication channels.
- Lead the discussion. Involve clients or customers, industry experts, analysts and the media in a broader discussion about the threat landscape and how businesses or organizations should meet the challenge. [20]

Make sure you comply with federal and state laws on whom to notify when a breach occurs. Once the vulnerability has been repaired and systems are operational, these are the next steps you should take in the "calm after the storm."

4. Conduct a postmortem.

There are three elements to be analyzed in this postmortem:

- Cause of the breach
- Incident response plan
- Communication plan

Cause of the breach. The forensic analysis should have uncovered the mechanics of the attack, vulnerability exploited and the damage done.

Incident response plan. Was the plan effective? Were there unforeseen circumstances not addressed? Were the response roles and responsibilities laid out clearly? Were its outcomes achievable? The plan can be modified as the organization learns from the breach. If an incident response plan was not in place, the incident can be used to create a framework with the understanding that it will need to be modified regularly.

Communication plan. All companies and organizations should have a communication plan in place so information can be disseminated quickly, efficiently and completely. If you have such a plan, evaluate whether it was followed and, if so, whether it was effective. Adjust if needed. If you did not have a communication plan in advance of the breach, this postmortem can help you develop one. If the breach was made public, media and public response should be analyzed.

Security monitoring service Threat Stack advises that security postmortems be “blameless” by making it clear that individuals are never the root cause of a breach. If an employee is blamed for an incident, everyone in the organization may be less willing to report suspicious incidents or potential security compromise. The postmortem should focus on why something happened and how to prevent it in the future.[21]

5. Identify future prevention measures.

The postmortem may reveal gaps in security, processes and/or personnel that should be addressed. Prioritize them in order of the risk to your organization.

Qualys, a provider of cloud security services, says these factors should be used to prioritize risk to IT assets:

- The importance of the role they play in critical business operations
- Their level of interconnectedness with other assets in your IT environment
- The level of exposure to the internet via web and mobile apps
- The size and nature of their user base[22]

Identify the best mitigation for each. Create a plan and a timeline for working through this list of priorities. This may involve budgeting for hardware, software and services. Designate a point person to manage this process or contract with a vendor.

6. Complete the reporting protocol.

The results of the investigation should be reported to all stakeholders in the organization. Network vulnerabilities should be reviewed, as well as the plan and schedule for mitigating those vulnerabilities. If the breach or the enterprise is subject to regulations related to incident reports, review these requirements and whether they’ve been fulfilled.

When the breach is internal.

While we think of cyberattacks as coming from the outside, there's another form of attack that's just as pernicious: employee data theft. An employee doesn't need to crack into the network or systems; sometimes it's as simple as plugging a USB drive into a company computer and copying files.

A common occurrence is a staffer taking intellectual property when he or she moves to a competitor or starts an independent company. In such a case, digital forensics can uncover the theft and provide solid evidence that can be used in court.

According to D4, The Adecco Group company Special Counsel's eDiscovery solution, the organization should involve a wide range of internal personnel, whether or not a forensics company leads the investigation.

Managers

The employee's manager is often the first person to become aware of the alleged data or information theft, so he or she must immediately follow incident reporting protocols. The manager should make note of the employee's duties and responsibilities, as well as establish a timeline, according to D4.[23]

Human Resources

In some organizations, the Human Resources department is responsible for conducting internal investigations, or it may be the main point of contact for external forensics investigators. It must act in a way that can withstand a legal challenge from the subject employee while maintaining that person's privacy and keeping the investigation confidential.

Inside or Outside Counsel

The organization's legal representatives must be kept informed so that they can decide, based on evidence uncovered, whether or how to proceed with legal action. For example, the evidence of stolen trade secrets or intellectual property may be strong enough to file a temporary restraining order.

IT

Personnel in the information technology group provide investigators with an understanding of the organization's information systems, including email, networks, mobile devices, cloud-based data, external media usage and company-provided devices and usage. The IT team must make sure that potential digital evidence, including metadata, is preserved.

All of these groups must collaborate with each other, as well as with the forensic examiner, in order to conduct a thorough and forensically sound investigation that will stand up in court while protecting the interests of the organization.[23]

Hardening the network

As we've seen in high-profile cyberattacks, almost anything can provide entry to ambitious criminals. A company can't secure every DVR, flash drive or HVAC service in the world. What it can do is adhere to security standards and best practices.

As you're recovering from a breach and ahead of the major work of upgrading cybersecurity, review your current network security measures to make any necessary changes.

Antivirus

Antivirus applications should be installed to protect the network at its three layers: the periphery, the server level and the client level, which may include not only desktop machines but also enterprise or brought-in mobile devices.

At the periphery, all possible entry points should be identified and secured. This may include connected infrastructure or devices such as smart thermostats. All traffic entering the network through these entry points should be routed through an antivirus gateway application.

At the server level, a best practice is to install antivirus software on each server and internally, both at the client (desktop computer) level and the server level.

To make sure antivirus protection is active and stays current, a central antivirus server should be used to configure and scan servers and clients. Where possible, install application-specific antivirus products. Antivirus programs should be continually updated by the vendor or service provider. Servers and workstations should be scanned daily at a time when this is least likely to interrupt operations or use.

Hardware and Software

If there is hardware and/or software in the organization that has reached end of life and is no longer supported, it should be upgraded.

Software should be updated and patched regularly; ideally, patches should be applied as soon as they become available. In order to effectively keep software updated, you need three capabilities:

1. Scan the network for all connected devices and detect the status of their operating systems and software.
2. Detect the current patch status of all applications.
3. Collect, configure and apply software patches without creating conflicts.

Take advantage of automatic software updates provided by their vendors. A patch-management service or solution can ensure that software stays up-to-date.

Application Whitelisting

This practice helps to keep computer systems safe from malware by denying access to any applications that have not been specifically approved by whitelisting. Whitelist software automatically checks new applications entering the system to see if they match the whitelist; if they don't, access is denied. This approach is more secure than blacklisting applications. However, it requires extra steps from users who must request an application to be added.

Hardening the organization

The postmortem may identify gaps in organizational policies and processes, as well as in personnel.

Deborah Hurley, Associate Faculty Director in Cybersecurity, says diversity in disciplines is an important factor in cybersecurity, as well as diversity in gender and ethnicity. Management, legal, compliance, human resources and communications must contribute and collaborate on security. She says true security affects and should be a part of every part of the company.[24]

The goals should be to create a "security culture," according to Andrea M. Matwyshyn, a Professor of Law and Computer Science at Northeastern University. Security should be pushed from the top down and treated as a fundamental part of the company, she advises.[25]

According to Matwyshyn, the security response calls for nothing less than a top-down effort from the C-Suite, "where security is treated as a fundamental piece of the structures within a company, because information security is only as good as the weakest link." She said companies must have Chief Security Officers and vest them with sufficient powers and social capital to be able to articulate needs in terms of staff, training or other investments.

That culture of security should extend throughout the workforce. All employees should be educated on the risks to the company, why individual security functions have been implemented, best practices and common exploits such as phishing.

A HIGH-PERFORMING SECURITY TEAM MAY INCLUDE THESE ROLES:

Chief Information Security Officer (CISO)

Not all organizations have a designated Chief Information Security Officer. In many, the CIO or CTO handles cybersecurity. A CISO is responsible for developing an infosec program and implementing it. As a member of the executive team, he or she is a peer who can educate and persuade other C-level execs about the importance of cybersecurity and the best ways to achieve it.

Security Director or Manager

In organizations without a CISO, the Security Director/Manager is the lead for developing and implementing security. This person should have the same technical experience as a CISO. Moreover, it's important that the Security Director/Manager have direct access to C-level executives.

Security Architect

The Architect designs the systems specified by the CISO or Security Director/Manager.

Security Engineer

Security Engineers implement the security systems and designs of the Security Architect. Their work includes upgrading, testing and patching security systems. They're also responsible for maintaining them and testing them regularly. These staff are on the front lines of an organization's day-to-day security.

Security Analyst

A Security Analyst creates policies for the enterprise that will best protect it from threat and risk, and then evaluates whether current measures comply with security policies. The Analyst must identify new threats as they arise while evaluating whether current security measures remain adequate. He or she reports regularly on the performance of security systems. The Analyst also may make recommendations about security methodologies and products.

Systems Administrator

Managing user accounts, passwords and access to IT resources are among the jobs of sysadmins, making them an important part of the security team. They also maintain antivirus protection, firewalls and application blacklists and whitelists.

How innovation will change the training and role of security professionals

Cybersecurity Ventures predicts that there will be a shortage of 1.5 million cybersecurity professionals by 2021, while there were 1 million open jobs in 2016.[26] Meanwhile, the work of these cybersecurity professionals has changed and will continue to over the coming years.

The Department of Homeland Security's National Initiative for Cybersecurity Careers and Studies is tracking new kinds of jobs and providing training and certification to fill them. For example, a Cyber Security Threat Intelligence Researcher sets up honeypots and sinkholes; uses a variety of tools for testing and evaluating malware; and hunts down the actors behind an attack.[27]

Artificial intelligence and machine learning are perhaps the most transformative technologies of the coming decade. AI will be a core differentiator among companies, providing improvements in processes or performing tasks that were previously impossible.[28]

The efficiency and massive computing power of AI will inevitably be harnessed by criminals. According to the Harvard Business Review, AI-enabled cyberattacks will bring hacking to a desperate new level.[29] In fact, artificial intelligence systems themselves might be hacked, subverting their intended purposes and using them to launch even more sophisticated exploits.

Companies that aim to use AI competitively will need to hire experts who can develop ways to ensure that artificial intelligences will perform in their owners' best interests and be protected from intrusions or exploits.[30]

At the same time, AI can be used to enhance cybersecurity. For example, an AI system can constantly check all an organization's systems for signs of intrusion, detect warning signs of insider threats and constantly monitor for violations of security policies. Experts will need to design, implement and manage these super-intelligent security systems.

Prepare Today For the Future of Cybersecurity

With the explosion of connected devices and the continuing expansion of the Internet of Things, the attack surface for any organization will continue to expand. At the same, new technologies such as artificial intelligence will demand new capabilities from the enterprise—as well as new expertise.

Businesses must come to terms with the fact that security can no longer be implemented and then simply maintained. Security practices and products must continually be updated, evaluated and improved under the direction of domain experts.

At Modis, we can be your partner in identifying skill gaps among current cybersecurity staff, determining new responsibilities and roles, and hiring experienced, exceptional IT talent to make your IT strategy a reality. To learn more or get detailed information about salary ranges, job descriptions and market demand, please contact your local Modis representative today.

Sources

1. http://cybersecurityventures.com/cybersecurity-market-report/
2. http://opim.wharton.upenn.edu/risk/downloads/WEF_Global-Risks_2017.pdf
3. https://ww2.frost.com/news/frost-commentary/cybersecurity-aftermath-ransomware-attack-what-lies-ahead/
4. http://www.pandasecurity.com/mediacenter/malware/adylkuzz-new-virus-wannacry/
5. http://www.bbc.com/news/technology-40428967
6. https://www.globalsecuritymag.com/WannaCry-What-s-Next-expert,20170518,71206.html
7. http://www.gao.gov/highrisk/overview
8. https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal
9. http://www.eweek.com/enterprise-apps/businesses-keep-clinging-to-windows-7-and-xp
10. http://analysis.tu-auto.com/telematics/can-you-hack-it-securing-connected-car
11. https://www.wired.com/2017/02/hacked-android-phones-unlock-millions-cars/
12. http://www.techrepublic.com/article/4-questions-businesses-should-be-asking-about-cybersecurity-attacks/
13. http://www.cnbc.com/2017/05/19/new-hacking-threats-fingerprint-vulnerabilities-and-sophisticated-ransomware.html
14. https://ioactive.com/pdfs/IOActive_HackingCitiesPaper_cyber-security_CesarCerrudo.pdf
15. https://blog.surfwatchlabs.com/2016/09/08/short-selling-vulnerabilities-latest-in-string-of-stock-market-manipulation/
16. https://medium.com/@RPublicService/feds-at-work-bringing-cybercriminals-to-justice-7dfe5d7a5920
17. https://www.gartner.com/smarterwithgartner/prepare-for-the-inevitable-security-incident/
18. https://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf
19. https://digitalguardian.com/blog/data-breach-experts-share-most-important-next-step-you-should-take-after-data-breach-2014-2015
20. https://digitalguardian.com/blog/data-breach-experts-share-most-important-next-step-you-should-take-after-data-breach-2014-2015
21. https://blog.threatstack.com/how-to-conduct-a-blameless-security-post-mortem
22. https://blog.qualys.com/news/2017/01/17/overwhelmed-by-security-vulnerabilities-heres-how-to-prioritize
23. http://d4discovery.com/discover-more/involved-with-conducting-corporate-investigations
24. https://www.forbes.com/sites/ciocentral/2017/05/07/improving-cybersecurity-the-diversity-imperative/#639ce3571e30
25. http://knowledge.wharton.upenn.edu/article/massive-global-cyberattack/?
26. http://cybersecurityventures.com/jobs/
27. https://niccs.us-cert.gov/training/search/cybertraining-365/certified-cyber-threat-intelligence-analyst
28. Menalto Advisors, Menalto Advisors Thought Report: Artificial Intelligence and Machine Learning.
29. https://hbr.org/2017/05/ai-is-the-future-of-cybersecurity-for-better-and-for-worse
30. http://www.businessinsider.com/deepmind-has-hired-a-group-of-ai-safety-experts-2016-11