OLIVER WYMAN

EMBEDDING CYBER DEFENSES WHERE THEY MATTER

AUTHORS
Paul Mee, Partner
Chris DeBrusk, Partner
Kenan Rodrigues, Partner
James Cummings, Senior Advisor

MARSH & McLENNAN COMPANIES

EXECUTIVE SUMMARY

The release of details regarding exactly what happened with the Equifax breach and the revelation that the SEC EDGAR database was hacked and the information it contained potentially used to support insider trading, represent a critical time to pause.

There are important learnings from each breach announcement and, as demonstrated by the most recent high-profile cases, they all have different underlying root causes and implications. In the case of Equifax, we have been reminded of the importance of focusing as much on security within the corporate network as we do on protecting entry in the first place.

"National security needs safe commercial and financial systems"

Given the accelerating frequency of breach announcements and the fallout that occurs when discovered, the historical approach taken by many organizations to addressing known weaknesses is simply not working. Beyond organizational cyber resilience, national security needs safe commercial and financial systems. It is worth taking a step back and considering what these events or other major data hacks in the recent past mean for the way in which corporations think about cyber risk and cyber defense.

In the aftermath of the publicity surrounding the Equifax event, CIOs and CISOs have been scrambling to assure their CEOs and Boards that they have things under control and aren't going to fall victim to the next major attack. Or, that they haven't already fallen victim and don't yet know this. Our premise is that many corporations need to consider fundamental changes in approach to cyber risk that goes beyond their current endeavors.

There are six key practices – that both address recently exposed weaknesses as well as fundamental changes beyond – that leading companies are now taking to improve their cyber defenses:

1. Move beyond a castle-defense model
2. Harden your data assets
3. Migrate from APIs to secure APIs
4. Don't just secure, verify
5. Make security a primary design requirement
6. Upgrade your cyber risk culture and accountability structure

1. MOVE BEYOND A CASTLE-DEFENSE MODEL

The traditional approach to cyber security is the perimeter model, or castle-defense approach. The logic being that if you harden the shell and build the "castle walls" high enough and thick enough, you can keep the marauding army that is the hacker community out and away from your treasure – this being predominantly the organization's data. While conceptually a solid approach, the hard reality in most large corporations is that their network environments are so complex (and the understanding of that complexity so low),

that it is nearly impossible to ensure that someone hasn't left the equivalent of a door open somewhere, or won't do so in the future.

A much more worrying challenge is a nation state attack. Until recently, hackers were generally lone wolves or worse, a small pack of wolves working to profit from ransom, extortion, or fraud. Today, there are direct and proxy-government organizations playing the offensive hacking game and they come with essentially infinite resources and the latest tools and information on zero-day vulnerabilities. It is a rare corporation that can ensure that a nation-state sponsored actor won't breach the perimeter eventually; irrespective of the level of cyber defenses they have in place.

Finally, there is a key cyber threat vector that is nearly impossible to fully inoculate against attack – employees. People are consistently the weak link in the cyber defense chain, being subject to phishing attacks, social engineering and occasionally just going rogue. Given that you need to allow your employees to operate within the castle walls to do their jobs, they are yet another area of cyber risk that needs to be considered and continually assessed.

It is therefore vital that organizations move beyond the castle approach and assume hackers will get in (and may already be in) and start to harden the internal systems, processes and databases in the organization so that if someone does sneak in via an external door, there is nothing for them to do other than wander down long hallways full of locked internal doors.

It is also critical to identify corporate assets that are of high value to a hacker and need additional protection. Forward thinking corporations are performing risk assessments on their systems and data assets with the goal of identifying those that represent the most attractive targets. These assets are put behind additional layers of network protection, user identify verification, and encryption to further protect them. While this improved protection can introduce some friction into business processes, often the risk-reward tradeoff is worth it given the potentially massive and publicly visible losses that can result from a cyber-event.

2. HARDEN YOUR DATA ASSETS

While it conceivable that hackers are simply aiming to cause damage by corrupting or destroying systems, it is more likely that they are after information, either to sell or to use for blackmail against the corporation, or in the case of a nation state attack as leverage over the country in which the company operates. By grabbing sensitive information, and either selling or releasing it, hackers can achieve their goals of direct or indirect financial gain, creating embarrassment and generating chaos.

IF IT IS THE DATA THAT HACKERS WANT, IT IS IMPORTANT TO PROTECT IT.

The large majority of data in corporate environments is not fully encrypted or protected by strong, tough-to-beat security infrastructure, processes and procedures. In fact, such data is more commonly protected by a single database password that is encoded into the applications that access the data. This situation exists primarily on the assumption that hackers would not penetrate the castle walls, so little thought was historically put into protecting data, beyond implementation of field level encryption for critical personally identifiable information (PII) such as social security number.

Often worse, the data that sits in these databases is then extracted into many different forms via a mix of processes and frequently informal arrangements, across Excel, MS Access databases, and other means difficult to fully protect. Data is often emailed, which means it is essentially unprotected and free for anyone who is rummaging around in the corporate network to steal.

With all this in mind, it is critical that organizations start locking down data assets in all forms via controls, monitoring, and encryption.

- Encrypt all data at rest – not just key elements like social security numbers but everything. Lock down data from access while tightly managing cryptography keys.
- Stop allowing data to be extracted and stored in easy-to-hack formats. Arguably, anyone can break into an Excel file, even if it has a password. Actively prevent valuable data from being stored in file systems, SharePoint® and other repositories while making sure you know exactly how they are secured and who has access. Even then, aim to minimize their use.
- Look to adequately protect data in motion as well. When hackers realize databases are fully encrypted and impenetrable, they are going to focus on tapping data moving between systems. Encryption used to be computationally expensive and therefore was avoided in the design of system interfaces. This is no longer the case, so strong encryption for data in motion needs to become the default.
- Analyze legacy systems to understand the cyber risk they create. Any system that is more than two or three years old was probably not designed with strong data protection and cyber security in mind. It is critical to understand where the real risks lie and develop strategies to protect data a given application creates and stores.

3. MIGRATE FROM APIS TO SECURE APIS

One of the key trends over the past 10 to 15 years has been a move towards service orientated architectures (SOAs). This approach breaks a business into functional components, supported by corresponding technical capabilities. Each "block" in the overall architecture talks to other blocks via application programming interfaces (APIs), and many times these architectures extend beyond the walls of an organization so they can interface to customer and third-party systems. The advantage of the approach is that rather than a given technical environment being a series of monolithic blocks of capability, it becomes a network of services that can talk to each other, and therefore be leveraged and reused in lots of ways. SOAs are more flexible, typically more future-proofed and can be less expensive to maintain.

What was often left out of the design of the protocols that allow the components of a SOA to communicate via application programming interfaces (APIs) was security, or a sufficiently strong security capability was not implemented. Data moved unencrypted and often without strong authentication and identity verification to ensure only truly validated systems were allowed access to the data.

It is time for corporations to reevaluate their system-to-system communications to ensure that they are secure and encrypted, consistent with the associated security risks. It is important to ensure that if a hacker gets past the perimeter, they cannot install a skimmer on this communication and simply copy transaction data for their own use.

A key question that CEOs need to ask their CIOs is whether the corporation has a map of all point-to-point movement of data, and if such a map exists, is the cyber risk associated with each data element known. If such a schematic doesn't exist, it needs to be created.

4. DON'T JUST SECURE, VERIFY

According to a recent report from FireEye, a security incident response company (www.fireeye.com), hackers spend an average of over two hundred days inside a corporation's network before they are detected. Based on the portrayal of hackers on popular television programs and in films, one might conclude that most hackers quickly break into a corporation's network, snag the data, do the damage, and get out. The reality is that hacking is often a game of patience and hackers will carefully step into a network, exploring, testing and learning. They will also install additional back doors in case their primary way of getting into the network is subsequently closed.

If you assume hackers will get in, and they will, then you also need to think through how you are going to catch them once they get in. There are a range of monitoring and surveillance solutions that can be deployed inside a computer network to identify and report on abnormal activity, system access, and other potential threats. It is also important to think of your internal network as a series of rings, with the most critical systems and databases sitting in the center and protected by multiple layers of security.

Not unlike the castles of old, where an attacker who breached the outer walls would find themselves funneled into tighter and easier to defend passages, a corporate computer network needs to be harder to penetrate the closer a hacker gets to critical assets.

5. MAKE SECURITY A PRIMARY DESIGN REQUIREMENT

In the modern business environment, organizations are actively and aggressively digitizing themselves to get closer to their customers and as a result, coupling their capabilities, internal processes, applications and data to their customer's systems. To achieve a more fully digitized organization involves opening up new doors in the castle walls thus creating more potential places for hackers to sneak into the fortress. It also involves exposing more critical data to your employees and third parties through digital means, which exposes the organization to potentially damaging actions by rogue actors.

When an application or system is designed and implemented, security can often be the last non-functional requirement that is addressed. It can be an afterthought and as such, isn't built into the core of the application from the time the first line of code is written. As a result, data in motion isn't secured, sophisticated risk-oriented access controls aren't implemented, and effective monitoring and logging to spot potential breaches isn't built into the application.

Given the cyber threat environment in which we live, where a new cyber event is announced almost daily and the average cost of a data breach is $3.62 MM according to the 2017 Ponemon Cost of Data Breach Study, cyber security needs to be the first consideration when implementing a new application or installing new vendor software.

As noted above, this is even more critical as corporations execute major digitization initiatives and more fully open up their systems and databases to customers.

6. UPGRADE YOUR CYBER RISK CULTURE AND ACCOUNTABILITY STRUCTURE

Perhaps the most important and most difficult part of improving a company's ability to defend from cyber-attacks is based less in technology and more in culture. Cyber risk is an ever evolving issue with new exposures and attacks emerging all the time.

Historically, cyber security was the purview of the CIO then it became a problem for all the newly minted CISOs. Now, with losses mounting and nation states getting into data theft as a way to make money or cause chaos and pursue their political interests, fully understanding cyber risk, and even more importantly taking steps to manage it, should be a top concern across the executive leadership team. **The problem is too large and complex for any single executive or group within the organization to successfully address.**

It is critical that the CRO, CIO, and CISO partner and collaborate to take the lead on meeting the challenge-leveraging their respective areas of expertise, with strong support from the CEO and the Board. However, in order to drive true cultural change, it is equally important that accountability is shared by all business leaders as well. **CIO, CISO and Technology can recommend and implement, but unless policy allows them to enforce and impart or directly influence employee and corporate actions, it won't be effective.**

The entire organization needs to participate in lowering its cyber risk profile, across all aspects and all levels of the enterprise.

Cyber risk needs to become top-of-mind at all levels of the organization, from the call center representative questioning whether the person they are talking to is actually who they claim to be, to the benefits manager considering whether the email they just received is actually one they should open, to the IT support professional thinking twice before reacting to the urgent call they received demanding that a password be reset immediately.

****

Protecting the company is much more than installing the latest firewall or virus scanner, because people are both a key risk and the key asset in reducing overall cyber risk.

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

AMERICAS
+1 212 541 8100

EMEA
+44 20 7333 8333

ASIA PACIFIC
+65 6510 9700

www.oliverwyman.com

OLIVER WYMAN