Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 15, Issue 6

A Holistic Approach to the Future of Cybersecurity

By: Stewart Collier

For many people, mentioning the term cybersecurity typically conjures up the Hollywood vision of an individual in a dark room running sophisticated code and typing furiously on a keyboard to access critical government data or to steal money from big financial institutions. This vision, though, is not reality. The truth is that cyberattacks come in a variety of shapes and sizes, from highly sophisticated and potentially state-sponsored initiatives like Stuxnet or NotPetya to arbitrary probing done by individuals with limited resources. In fact, the 2018 Verizon Data Breach Investigations Report found that 58 percent of data breach victims are small businesses whose cybersecurity vulnerabilities are exploited by automated attacks designed to probe at random.

As a result, most enterprise breaches are not the result of cyber criminals inventing new, high-profile ways of doing damage. Rather, they are due to shortfalls in the development and enforcement of holistic, layered security processes and protocols. Many enterprises in the US and across the world buy into the myth that buying and installing software like antivirus programs or machine learning platforms can keep them safe. Unfortunately for them, this couldn't be further from the truth: software is but a tool to support a comprehensive cybersecurity plan. From my perspective, a strong cybersecurity strategy must revolve around establishing the right combination of physical protection, quality assurance, regulatory compliance and client buy-in to overcome present and future cyber dangers. In this article, we will examine the following topics:

- Common gaps in enterprise cybersecurity practices
- How to approach the resolution of cybersecurity weaknesses
- Emerging trends in cybersecurity and what enterprises need to watch out for in the future

Although I come to this article from a large data center provider perspective, the topics discussed are applicable for all sizes of organizations, whether they run their own on-premise data centers or contract with a third-party provider. At the end of the day, the integrity and safety of the data (and that of their customers) is what matters most, and that is why there is a country-wide necessity to think bigger picture.

When it comes to identifying gaps in cybersecurity, it is often a lack of basic security protocols combined with a failure to think holistically about IT assets and business continuity that gets enterprises in trouble. Here is a brief list of just some of the issues that I witness the most:

Weak Password Utilization

While having strong passwords is a basic aspect of a good cybersecurity strategy, many organizations often do not do enough in terms of company-wide training to establish password best practices. In fact, I have seen many individuals either using the same password for multiple protected files or programs or failing to change passwords regularly. While an often-cited best practice for refreshing passwords is 90 days, I personally prefer a 30-day window. This is because enterprise data breaches do not always come from the outside, yet another misconception that lands companies in hot water.

Assuming Attacks Always Come from External Sources

While high profile attacks from outside hacking groups like Anonymous or Fancy Bear get a lot of attention, insider threats can account for up to 75 percent of data breaches. Sometimes a breach can be the work of an unhappy employee looking to leave a mark on the company he or she dislikes. At other times, it can be simply the result of an employee's lack of training as to his or her role in upholding the company's cybersecurity plan and goals. In fact, at a recent Black Hat security conference, organizers reported that up to 84 percent of all cyberattacks are due to human errors such as failing to apply a patch, using weak passwords or even leaving devices unlocked in unsafe areas.

Lack of Business Continuity Mindset

Because many organizations either think they might get away without being targeted or that there is a fix-all program they can install to protect themselves, they often do not spend enough time thinking about what their response should be in the event of a cyber attack. For example, with the rise of social engineering attacks such a scam emails disguised as legitimate correspondence from reputable institutions, the risk of attacks is only increasing. According to FireEye researchers, for example, one in every 100 emails sent around the world is meant to deliver malware or commit a cyber crime. So, while company-wide training and planning is important to minimize the risk of an attack occurring, organizations need to ensure a plan is in place to deal with the aftermath of a successful attack and ensure their data is still accessible.

I like to think about the likelihood of a successful cyber attack like this: if someone is dedicated enough to target an enterprise and is willing to go all-out in order to make it happen, the best technological tools available on the market may not be enough to mitigate the risk of a successful attack actually taking place.

Thinking Holistically About Cybersecurity and Compliance

Cybersecurity needs to start with the top down. When I work with customers, I always start with a gap analysis where we review, over a three-month period, all aspects of cybersecurity that are relevant to them. Once that review is complete, however, it is important to ensure that there are significant leadership stakeholders within that enterprise who are willing to buy in to this paradigm. After all, security is a combination of protocols, programs and training, not simply the deployment of a tool like an antivirus program or an AI-based security application. Having an executive who can own and champion the cybersecurity paradigm for the organization is critical.

Once a company's leadership is truly on board, cybersecurity starts with the physical. Whether a company operates its own on-premise data center or relies on a third-party provider, here are some best physical security practices applicable to both:

- 24/7 video surveillance of the data center with an appropriate footage archive
- Multi-factor access control involving key cards, locks and biometric authentication, with the ability to add such protection incrementally

- Required presentation of government-issued photo ID for all visitors
- Constant testing of all physical controls
- Annual Threat Risk Vulnerability Assessments with remediation planning
- Periodic employee Security Awareness training

Of course, for full effect, these protective measures need to be coupled with a strong emphasis on ensuring full compliance with applicable regulatory standards. In my view, compliance regulations are an underrated yet extremely valuable component in minimizing the risk of human error and guiding an enterprise's internal security initiatives.

The Move to Global Compliance Frameworks

Meeting compliance mandates not only ensures maximum security and availability but also enhance an organization's reputation in the eyes of its clients. Here is a list of the most common standards that organizations and third-party data center providers should be compliant with, depending on the sectors in which they are involved:

- NIST 800-53PE and FISMA
- SSAE-18 (SOC1) / ISAE 3402
- PCI DSS
- HIPAA
- HITRUST
- ISO27001

Although all of these are important, ISO27001 is one of the main compliance standards I like to promote, mainly because it is a global standard as opposed to a US-centric one. For those who may be unfamiliar with it, ISO27001 is a technology-neutral framework that is designed to assist enterprises in establishing, maintaining and improving an information security management systems (ISMS). Overall, ISO 27001 brings information security under management control and gives specific requirements that, if met, are awarded with an accredited certification. As a result, it fits with the overall paradigm that cybersecurity is a question of overarching management processes and not just technical IT solutions. Think back to 1970 when the US government passed the Occupational Safety and Health Act, making employers legally accountable for providing employees with an environment free from identified hazards. In a similar fashion, global frameworks like ISO27001 are doing the same for the field of cybersecurity.

The Future of Cybersecurity in An Increasingly Connected World

While layered physical security protocols ultimately form the backbone of strong security programs, it should be noted that modern technological applications like machine learning and AI do have their place in protecting an enterprise from cyber attacks. Offered by myriad key players in the information security sector, machine learning essentially trains algorithms to identify a baseline for a system and flag unusual activity for human review and intervention. From our perspective, however, if companies can build machine learning systems to block attacks, so too can cyber criminals in order to probe and test suspected vulnerabilities. As a result, machine learning remains best conceptualized as a tool, and not a cure, for enterprises that need to strengthen their cyber security strategies.

More importantly, however, the entire landscape for data protection is beginning to change as the adoption of Internet of Things (IoT) compatible devices continues to skyrocket in the US and across the world. According to Cisco, by 2020, over 50 percent of the world's 28.5 billion devices will be machine-to-machine (M2M) connections for IoT applications. Most interestingly, 14.6 billion of these connections will be for devices like smart speakers, fixtures and other devices common to our homes and offices. As data processing and storage for these IoT-connected devices moves closer to the edge, cyber security will become more challenging for two reasons. First, most IoT devices lack traditional IT hardware protocols and are not set up to receive regular updates and patches like

conventional computing programs. Second, today's devices encompass such a diverse set of use cases that it becomes difficult to track potential threats.

Think about it: we are now seeing an influx into the marketplace of IoT-compatible devices that can automate our homes, offices and vehicles, as well as monitor and advise on our personal health statistics. All the data they generate is being increasingly stored in edge servers that reside outside the secure walls of traditional data centers and public cloud server farms. Additionally, these edge servers are often managed at a distance, without much attention paid to vital physical security practices. As Network Computing recently noted, "ensuring edge computing security is much more challenging than providing cloud security due to the fact that edge computing involves distributed data processing." When coupled with the typical, pervasive cybersecurity gaps we encounter regularly, this can pose an even greater risk to the integrity of an enterprise's data.

So, what does all this mean for enterprises as we move into 2019 and beyond? Basically, it means that taking a holistic approach to cybersecurity is more important now than ever. No enterprise can ever fully be protected from a potential attack; the trick is to work to minimize the risk of an attack occurring as much as possible and to have a business continuity plan in case it does happen. Train your staff on best cybersecurity practices and communicate regularly with them about new threats and how to respond. Most importantly, think about partnering with cyber security consultants and third-party data center providers with a proven track record of employing multi-layered, stringent cybersecurity protocols and being compliant with global standards like ISO27001 and others. Taking a holistic approach to your security strategy is the best way to protect your valuable enterprise data.