Balancing the risks and challenges in cybersecurity

Chief Information Security Officers (CISOs) and their security teams today face unprecedented challenges as they try to keep up with increasing threats to the business. Cybercriminals continue to evolve their tactics in creative new ways that often leave organizations in a reactive state, looking for more and more solutions to add to their security stack. But, more is not always better.

There's no doubt that managing security today is a daunting task. Security teams try to be a jack of all trades and but end up master of none. Many don't even have a clear understanding of the potential impact an incident could cause. It's no wonder organizations struggle to find just the right balance between the vast variety and complexity of threats they face and finding the right solution through a variety of challenges.

On one side of the scale, threats

Today's threats are vast. IBM's 2018 Cost of a Data Breach study finds that in the U.S., the average financial impact of a single data breach is $7.91 million. And, on average, it took companies 197 days to identify a data breach and 69 days to contain it.[i]

The drivers that contribute to the cost of a data breach include:

- Detection and escalation: Forensic and investigative activities, crisis management teams
- Notification costs: Communication with customers, regulators, and law enforcement
- Post data breach response: Offers for identity protection services, legal expenses, regulatory fines
- Lost business costs: Loss of customers and reputation, business downtime

And that's just identity theft incidents.

Distributed denial of service (DDoS) attacks and ransomware are close behind in the damage they do to the business. Denial of service, where hackers flood systems with so much useless traffic that it effectively stops the system from working, can stop a business in its tracks. While DDoS attacks most often bring down websites, one was recently used to disrupt the central heating systems in some buildings in Finland.[ii] The very fact that DDoS attacks are now so versatile is also what makes them so dangerous.

Lastly, ransomware, inserting a virus into a system and demanding some kind of payment to remove it, has also increased in impact and complexity. Cybercriminals are innovating at a fast pace in both technical and social engineering to try to stay ahead of the security measures intended to stop them. They then attack organizations that are most impacted by being offline, such as banks and hospitals.

While data breaches, DDoS and ransomware have been around for a while, the Internet of Things (IoT) has now created a new frontier for hackers that must be secured by organizations. In a most frightening example, the FDA required hospitals to stop using a particular infusion system that was administering medicines intravenously because it could be remotely accessed by hackers, allowing them to control the device and change the dosage it delivers.[iii] Given the rise in IoT and the lag in securing these devices, even more impactful incidents can be expected in the future.

On the other side of the scale, security challenges

The negative publicity from security breaches has definitely raised awareness with senior leadership, but the incidents still continue—and not just small incidents. It would be natural to think that this potential risk to the corporation would have organizations doing whatever it takes to secure the business. However, the threat landscape is a complicated and moving target, making it difficult to address every possible threat.

Some of the major challenges organizations face when trying to address security include:

Continually changing threats and regulations

Cybercriminals never stop evolving and innovating their tactics. As such, regulators are constantly adjusting and improving their requirements for security. What was once a strong security plan becomes quickly outdated as the ground continues to move. It's extremely difficult and onerous to try to keep up with the ever-changing security landscape.

Transforming to a more digital business

Digital transformation (DX) and connectedness, through technologies like the Internet of Things (IoT), cloud-based applications and mobile computing, has expanded the network beyond traditional boundaries and is producing a massive amount of data. Both of these have greatly increased the enterprise attack surface, raising cybersecurity risk. In the interest of providing quick value with DX, security measures tend to lag or not be considered at all.

Evolving IT infrastructure

IT infrastructure isn't stagnant either. Existing software needs updates and patches, new systems come online all of the time, and mobile and cloud environments only complicate trying to secure IT infrastructure. As the IT environment gets bigger, broader and more complex, many organizations lose track of where their risks and vulnerabilities are.

Inability to identify critical data assets

Businesses have so much data, that many don't have a good grasp on what data is critical to the business and where that data resides. And it's not just the data that needs to be inventoried and protected, but also who has access to the data. Additionally, identifying and protecting big data is not easy. It takes knowledge, funding and resources. However, not doing so can leave critical information vulnerable to security breaches.

Banking on compliance-driven security

Most every business has compliance regulations that must be followed. These regulations are put in place to protect the financial health of the business, its reputation, and its customers, among other

things. Meeting regulatory compliance standards can be a burdensome task leaving those who do so believing they have now secured their organization. Unfortunately, being compliant is not the same as being secure.

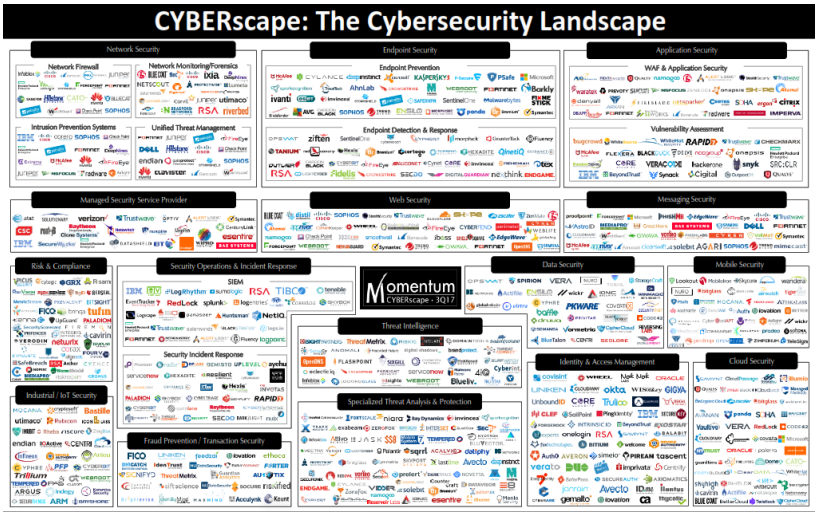
Over-reliance on annual audits

Annual assessments and testing are an absolute necessity, especially if the organization must comply with federal regulations. These annual assessments can be time consuming and resource intensive. While it's critical to check to see how security measures are working and whether there may be any gaps, checking the box annually does not equal true risk management and a secure organization.

> *[possible sidebar]*
>
> More than 60% of US companies globally cannot sustain compliance with PCI after initial achievement (Source: 2018 Secure Verizon Report)

Relying on point solutions from vendors

Layering more tools, resources and technology does not automatically produce an ever-ready security program. The security market is complex with hundreds of vendors and technologies insisting that their "must-have" solution will solve an organizations security challenges. Yet, when it comes down to it they do little to assess, diagnose and resolve foundational challenges and improve the organization's security program at its core.



Inadequate resources and budget

Lastly, with all of these security challenges, it's no wonder organizations struggle to find enough skilled resources and secure adequate budget and funding to support fully securing the organization. Waiting for new budget requests takes time and increases opportunity cost when staff could be mitigating risk. Many often schedule security work when it is convenient for them and not based on a budget cycle. Even with what should be an adequate budget, unplanned security threats and compliance regulations can impact an organization at any point within a budget year.

How to balance the scale

At its core, security risk has three components: threats, vulnerabilities and consequences. What the business needs to know is what could happen, how likely is it to happen to their organization and if it does happen, what are the consequences. Knowing the answers to these questions will help organizations work towards creating a security risk program that drives awareness, formulates an action plan and prioritizes security measures for key business processes and assets.

Wherever an organization is in its risk management maturity, it's never too late to go back and ensure the basic foundation is solid in order to balance the scale. Fortunately, there are best practices that can be implemented to help build a security program that is right for each business. These include:

Ensure awareness and understanding of security risk management

It's highly important to continually communicate and educate senior leaders about the changing threat environment, where and how it could impact the business, and what it takes to address the risk. The conversation should be two-way, with business leaders communicating the priority of critical business assets.

Prioritize and address high-risk business assets

Knowing where to focus time and resources will help ensure the most important business assets are protected and that those resources are used most efficiently. Start by identifying all critical systems and business processes and conduct a data mapping exercise to understand where sensitive data resides and its access points. Then, document current security capabilities and perform a gap analysis to identify and address security weaknesses.

Embed security risk management into the culture

A surprising number of security breaches occur because an employee did or did not do something to keep the business safe from intruders. Security measures must be embedded into the company culture. Employees need to learn how to prevent security attacks from things like phishing, sharing passwords, taking sensitive data beyond the secure perimeter, etc. Make continuous education for security a priority and employees will begin to live it.

Use existing best practice frameworks

There are many different security frameworks to protect different business practices and industries, such as PCI DSS, COBIT, ISO, NIST, etc. Rather than trying to build their own security program, organizations should start with the frameworks that are pertinent to the business. Although compliance regulations can prescribe some very strong security measures, remember, those regulations alone do not equal a secure organization.

Continually review and refine the risk management plan

Both the security threat and IT landscapes are fluid. New threats are emerging all of the time, business-critical applications are constantly being updated, and new applications are coming online faster than ever before. These landscapes must be repeatedly assessed and prioritized for areas of unexpected or excessive risk.

While all of these best practices will go a long way toward building a solid security foundation, the best plan is a plan that fits the particular business. There isn't any business that needs, or can afford,

everything. Organizations have to find the right balance of protection, not too much and not too little, that is in line with what is required by regulations and that provides the security needed to protect critical assets.

The ROI of just right

Adequate funding and skilled resources to support security programs are not always easy to come by. Calculating return on investment (ROI) for security programs can be difficult. But it is still critical to understand the benefits and be able to articulate that a robust security risk program is worth the time, money and resources to senior leadership.

One way that can help is to look at a cost-benefit analysis to understand potential cost savings over the cost of the program. Much has been written about the costs of security breaches and it's important to understand the potential costs an organization could face. These include replacing any damaged hardware, buying and using recovery software tools, recovery costs associated with the recovery, loss of productivity and reputational costs, and lost business. Identify a potential likely breach to the organization to use as an example to understand the cost savings of preventing a breach.

The cost side of the equation involves the people, technology, and time invested in protecting the organization. This should be relatively easy to quantify and justify. It is also where organizations should pay the most attention. Too little spent on security, the ROI looks good, but the company is not fully secure. Too much spent on security, the ROI becomes tough to justify and the company may be over or inefficiently protected.

Every business has different needs and its security program must be optimized to fit those needs. It should never be a "one size fits all" program. By understanding and prioritizing business risk, organizations can be sure that they are not overspending for protection they may not need. However, to understand this, the organization should conduct a security assessment that identifies potential threats, critical business assets and current capabilities.

[possible callout]

Sample Security ROI Metrics:

- % decrease of cost and speed-to-market of new, secure business initiatives
- % decrease of cost to demonstrate and maintain compliance
- % increase of operational efficiency (Mean time to detect / Mean time to resolve / mean time between critical incidents)

Fine tune the balance for optimal security

Many organizations either do not have the capability or the time to conduct their own security assessment and strategic plan. This is where they should enlist the help of industry experts. It's important to find a solution that is specifically geared toward helping organizations develop or optimize a solid security program that is customized to their specific data security needs and concerns.

The method that has proven most successful is to work with a security solutions provider that will provide a security strategy assessment of the organization's current security state, identifying any gaps and working to prioritize addressing those gaps according to business needs. The provider should dig

into an organization's current capabilities, identify what is working, what is duplicative and optimize the security program to prevent today's changing threat landscape from affecting the business.

With the strategy plan in hand, organizations should work with the security solutions provider to build strong and scalable security programs upon best-practice core essentials. These best practices will vary based on the type of industry, so the security program should be tailored to the individual business needs. Ongoing, they should work together to perform regular health checks, vulnerability scans and penetrations tests.

The speed and flexibility of the solution means organizations can meet changing needs throughout the year and new gaps in security can be recognized and remediated immediately. This saves time and money not having to manage multiple solutions and multiple vendors. And, it's important to work with a security solution provider that works with and can manage the world's leading vendors in the application security, data security, network security, endpoint security and security intelligence spaces.

Final thoughts

Trying to keep up with the ever-changing cybersecurity landscape can feel like playing the game of "whack-a-mole." Continually meeting compliance regulations while simultaneously responding to an increase in external and internal threats is extremely difficult for security executives managing tight budgets. Layering more tools, resources and technology does not automatically produce an ever-ready security program.

It's time for organizations to take a step back and make sure they have a solid, well-balanced security program customized to meets the needs of the business. Scalable and strong security programs are built upon best-practice core essentials that provide the foundation to protect and support organizations. Organizations should choose a provider that will dig into its current capabilities, identify what is working, what is duplicative and optimize the program to prevent today's changing threat landscape from affecting their business. Data security is not a one-and-done activity.

Take the next step

Essentials@Optiv provides CISOs with the ability to assess, prepare, manage and mitigate planned and unplanned security challenges – no matter when they need attention throughout the year.

Learn more about how Optiv Essentials can help your organization secure your business with a solid security foundation that is the right fit for your needs.

---

[i] 2018 Cost of a Data Breach. IBM. July 2018. Retrieved 12/19/2018.

[ii] DDoS attack halts heating in Finland amidst winter. Metropolitan.fi. November 7, 2016. Retrieved 12/19/2018.

[iii] FDA directed hospitals to stop using Hospira's Symbiq Infusion System. SecurityWeek. August 3, 2015. Retrieved 12/19/2018.