Top 5 Things Every CIO Should Know About Security

Anyone peeking into the mind of a CIO will see it swirling with questions. A tornado of limited resources, balancing security and technology, and feeling alone in it all obstruct the path to security success. What's worse is that the toughest challenges aren't related to technology—where CIOs feel most comfortable.

To help CIOs calm the storm and navigate through the journey of security, let's look at the top five things from an unconventional perspective:

1. **Security Isn't Your Fault**

   I'm afraid of being blamed if something goes wrong.

   Ask anyone within an organization where the security responsibility falls and you're likely to receive the same response—IT. While yes, IT identifies areas for security improvements along with technology and process recommendations, the answer is fundamentally flawed. CIOs need to know that while viewed as a "technology problem," security is a business problem.

   The business as a whole determines the level of investment through budgets, staffing, and prioritization of goals. If a phishing campaign is successful, it's not your fault. Being the victim of an attack is almost guaranteed these days. In the event of a successful attack, was there enough budget to purchase the necessary technologies? Was staff trained on cybersecurity best practices?

   There are many factors, but the bottom line is that businesses must decide what level of risk is acceptable. If the top priority is to increase revenue, it's likely that the business will limit security spend to an amount that provides "good enough" protection.

2. **Know How to Find and Get the *Right* Resources**

   All CIOs have access to resources, but not all resources are a good fit. For staff and budget, there is a clear line between the right and wrong resources.

   Staffing the *Right* Security People

   What if I don't have enough skilled resources?

   Let's face it, a good IT person is difficult to find. Layer in a security background requirement, and the pool narrows. The annual (ISC)² Cybersecurity Workforce Study concluded that globally, nearly three million security positions are open because of the cybersecurity workforce shortage.

For CIOs wanting to strengthen their security teams, recruit and keep professionals by following these guidelines:

- **Don't** post an entry-level job that requires five years of experience. Better yet, cross-check your job descriptions to make sure your ask is realistic.
- **Do** grow your talent organically. Especially if you can't afford a seasoned professional or what you're seeking is a unicorn that doesn't exist (yet).
- **Don't** forget that you get what you pay for. Be prepared to invest in hiring the *right* talent.
- **Do** make your security teams feel valued so that they don't leave for one of the three million open security positions.

Identifying an Appropriate Budget

What is an adequate budget for security?

Having an infinite budget means you can make anything happen. That's not the reality for most organizations. Budgeting requires CIOs to define the exact amount to dedicate to securing the organization. When under the pressures of the budget planning cycle, it can be easiest to refer to the previous year—using a small percentage of the overall IT budget for security. CIOs should resist this urge. Instead, use these guidelines based on the classic business justification:

- **Do** align the budget with strategic business goals and initiatives.
- **Don't** decide the budget based on a percentage of the IT spend.
- **Do** factor in the business risk appetite and daily security operations.

3. **Engage Service and Solution Providers You Trust**

How do I get beyond the sales hype?

Today's model for IT and security usually involves functions performed by a provider (penetration tests, risk/compliance assessments, and augmenting staff functions). Given the shortage of cybersecurity professionals, organizations have become vulnerable to service providers that claim to be "security experts" and a level of service that does not match the contract.

To mitigate this risk, CIOs need to go beyond the sales pitch and vet all providers (references, years in business, certifications, etc.) and revisit contracts to ensure providers fulfill expectations. Since MSPs are now a prime target for malicious actors, not doing your due diligence exposes your organization to tremendous risk. In fact, the Ponemon Institute reported that 59% of companies have experienced a third-party breach in 2018.

4. **Understand What Regulatory Requirements Apply and How to Implement Them**

Does compliance actually help my organization be more secure?

PCI/DSS, GDPR, CCPA, HIPAA, DFARS—there are a plethora of compliance standards that require organizations to be secure. Using a security framework like NIST's will help you meet 80%-90% of the requirements. Yet, that does not mean that if you are in compliance, you are secure. While not being in compliance is a risk, the regulations are not a security program.

Maybe you have identified that the data your organization houses requires compliance to a regulations, but that data is "nice to have." Even if you remove the vector and move out of scope, you still need a security program.

5. **Know How to Balance the Priorities**

Which is more important?

Balance is the key to life and happy CIOs. Applying that to security, CIOs should prioritize based on risk. Again, we return to the business justification and risk appetite.

CIOs should start by gaining an understanding of the business goals and objectives and assessing the environment. Then, create and implement a plan includes security and technology from the beginning. In the process, be sure to use a sounding board because as humans, we can't know everything.

Reading the five points above is a good start to overcoming the toughest challenges a CIO faces. While we have answered some of the most common questions, there are still more to answer. Download our service brief on NeuEon's Cybersecurity Leadership Practice to learn how we can help ease your mind and achieve security rightsized for your business's risk appetite.