How Security Fits Inside the Mind of a CIO

Answering the Top 5 Security Questions

neu·eon

The CIO's mind is swirling with challenging security questions. A tornado of limited resources, balancing security and technology, and feeling alone in it all—obstructing the path to security success. What's worse is that the toughest challenges aren't even related to technology—where CIOs have a lifetime of experience.

NO CISO?

ONLY 51% of SMBs have a top security executive

compared to

88% of enterprise-class organizations[1]

1 Will I Be Blamed if Something Goes Wrong?

Cybersecurity attacks are almost guaranteed these days, but CIOs aren't to blame.

WHAT PEOPLE THINK

- IT is Responsible for Security
- Security is a Technology Problem

REALITY

IT identifies areas for security improvements, along with the use of technology. The business determines the appropriate level of investment for protecting data and the business.

SECURITY IS A BUSINESS PROBLEM

1. The business decides what level of risk is acceptable and determines investment through budgets, staffing, and prioritization of goals.
2. Goals dictate investment decisions.

BOTTOM LINE

If something goes wrong, the onus is on the business. The business decides 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 What if I Don't Have the Right Resources?

Make changes to get staffing and budgeting "right." Having the right tools makes all the difference in getting the job done.

ATTRACT TOP TALENT

- Post realistic job descriptions
- Grow staff organically
- Prepare to invest
- Make your security team feel valued

3 MILLION OPEN SECURITY POSITIONS because of the skilled cybersecurity workforce shortage[2]

BUDGET "RIGHT"

Having an infinite budget means you can make anything happen. When does that happen? Never.

ALIGN
security budget with strategic business goals or initiatives

BOTTOM-UP ANLYSIS

- Tech
- Training
- Staff
- Managed Services

3 How Do I Get Beyond the Sales Hype?

The sales hype can be dizzying. With everyone staking the same claims and promises, CIOs need to find trustworthy service and solution providers by searching for reviews and press coverage, vetting references, and checking that certifications are current.

CONTRACT TIPS

- Revisit on a bi-quarterly basis
- Be careful of auto-renewing contracts

MSPS ARE A PRIME TARGET FOR MALICIOUS ACTORS[3]

because of privileged access to customer environments

59% EXPERIENCED 3RD PARTY BREACH[4]

choosing the wrong partner could put your organization in danger

For more detailed guidance on the challenges CIOs face, read our blog series, "Top 5 Things Every CIO Should Know About Security."

4 Does Compliance Actually Help My Organization Be More Secure?

Getting stuck in the compliance game is where companies go wrong. Meeting compliance requirements offers a false sense of security, but it doesn't address the entire organization.

COMPLIANCE ≠ SECURITY PROGRAM

USE SECURITY FRAMEWORKS LIKE

NIST Security Framework (CSF), ISO 27000 Series, or the "Top 20 CIS Critical Security Controls" to build security programs and meet **80%-90%** of compliance requirements

5 Which Priority is More Important?

When prioritizing security, CIOs should stay rooted in the risk-based view and utilize the business justification to define scope and expectations.

BALANCE IS THE KEY FOR HAPPY CIOs

- Bake security in rather than bolt on
- Plan the work, and work the plan
- Assess, address, monitor, and adjust
- Use a sounding board

Need help navigating the strategic complexities of a comprehensive cybersecurity approach?

NeuEon's Cyber Risk Leadership Practice helps move companies from frameworks and theory to practice, communicating up and down the organization to ensure your risk is addressed appropriately.

info@neueon.com
neueon.com
@NeuEon **NeuEon**
275 Grove Street, Suite 2-400
Newton, MA 02466
877-273-9200

Sources:
[1]https://www.idg.com/tools-for-marketers/2019-security-priorities-study/
[2]https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study
[3]https://www.us-cert.gov/ncas/alerts/TA18-276B
[4]https://www.ponemon.org/library/data-risk-in-the-third-party-ecosystem