CYBERSECURITY IS NOT A DEVICE

EFFECTIVE APPROACHES TO MANAGING CYBER RISK

By Brandyn Fisher

((CENTRIC))

EXECUTIVE SUMMARY

"Jamie" carries a challenging, daunting position at her highly reputable organization. She's in charge of "cybersecurity," whatever that means. She drew the short straw, and now her board of directors – made up of investment bankers, former C-level executives and current leadership – has set an expectation that it will not be the next company on the front page of the Wall Street Journal for having a major security breach.

"Are we secure?" they ask, expecting a confident response from Jamie. The answer to this looming question is never a straightforward "yes" or "no," and Jamie knows this, but how does she communicate that to her board?

It's complicated, complex, difficult to track, scary and expensive; it's a taxing burden. Jamie also knows this multifaceted problem can't be solved by simply buying another security device. It takes a programmatic, trackable, risk-based approach. It takes time and perspective. Like Jamie's board of directors, stakeholders in most organizations want the peace of mind that comes with confidently knowing secure practices are in place. Unfortunately, most may not be aware of all that is involved in getting there.

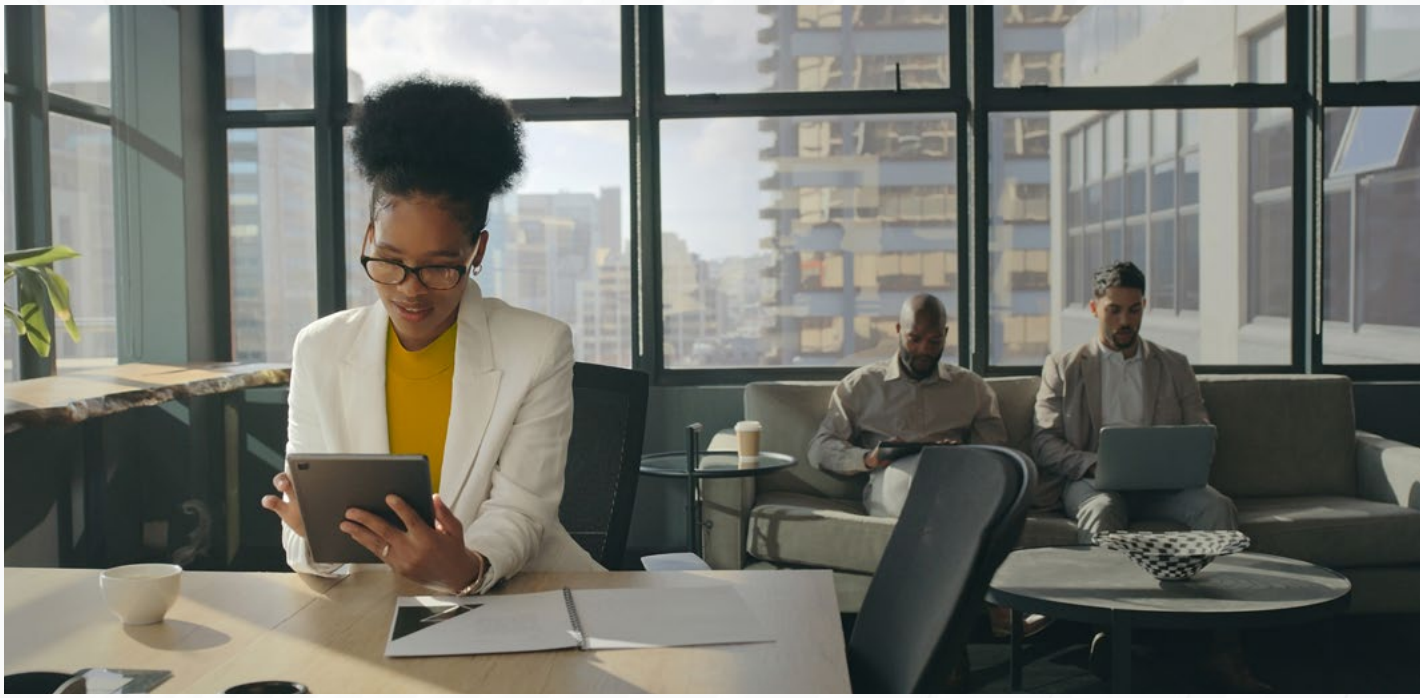
Cybersecurity remains one of the hottest points of contention when speaking to leadership, executives and corporate boards across the globe.

The problem: What is needed for a company to be "secure" varies greatly from one business to another, and no one seems to understand how to capture exactly what it is or how to manage it. Non-technical leadership is required to make business-sensitive, strategic decisions on cyber-centric matters, often with a lack of knowledge to make such conclusions. Through client trials, industry perspective and a benchmark for what "good" looks like, we're hoping to help simplify the equation.

COMMON CYBERSECURITY MISCONCEPTIONS

Through relationships with companies of varying complexities, we commonly find that leadership is uninformed and misguided. Most frequently, we find organizations that believe cybersecurity is a "box," such as a modern firewall, or a series of boxes. Perimeter defense, universally associated with a firewall of some sort, is of critical importance. However, while these items certainly are relevant and important to your overall cybersecurity program, they are a small portion of what it takes to manage your overall cyber risk. Devices are critical, but they won't prevent your name from ending up in the newspaper for the wrong reason.

While the idea that devices are the solution to cybersecurity management remains the most common misconception, we find many organizations also have complementary programs providing a false sense of security. Companies that are accountable to the public and must be compliant with the Sarbanes-Oxley Act (SOX) feel a false sense of security in the cyber arena. SOX is designed to implement and test controls that are deemed necessary to prevent a financial misstatement. However, many controls that are critical to a mature cybersecurity program exist outside the scope of SOX.

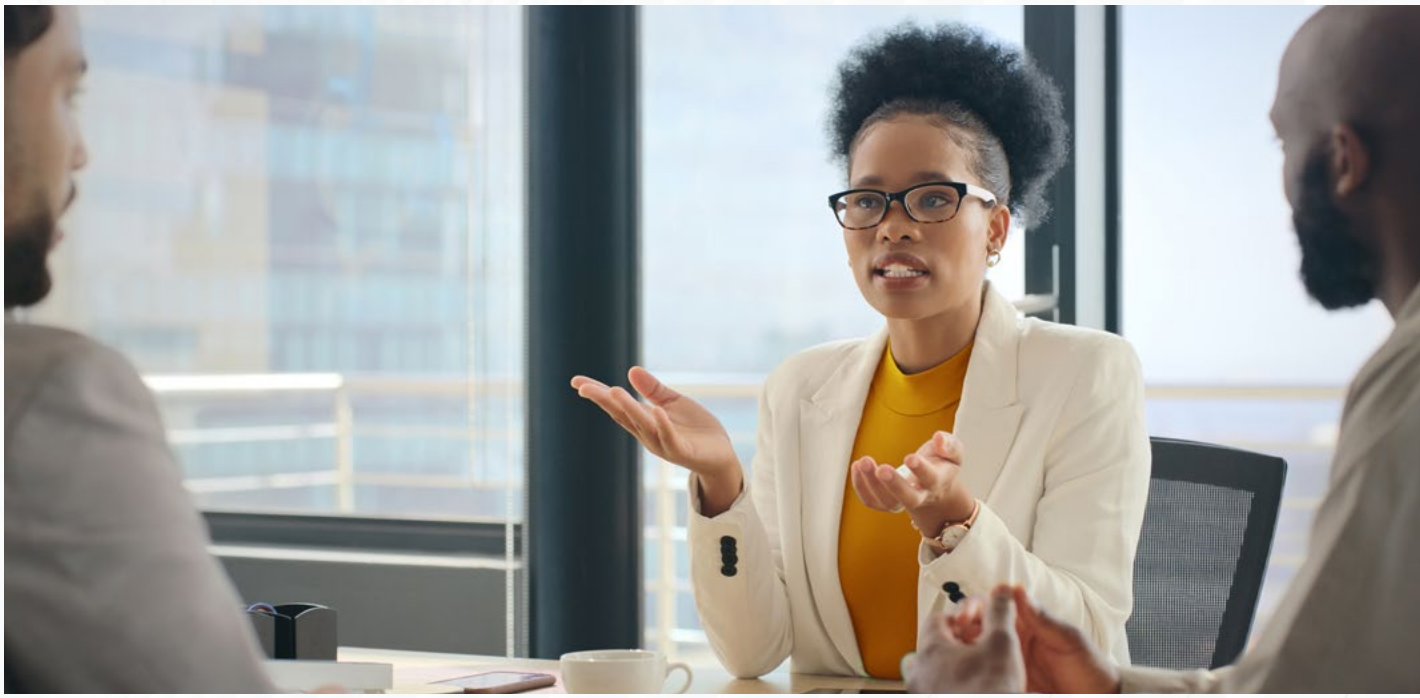


COMMON CYBERSECURITY MISCONCEPTIONS (CONTINUED)

Hacker, hacked, hacking – these scary words are top of mind for leadership and other decision-makers. Truthfully, the likelihood of being hacked from outside an organization is low. Unfortunately, organizations of all shapes and sizes overlook what happens within the walls of their respective entities. Internal threats are real, and they're far more common, easier to exploit and have a much higher value to cyber predators than external hacks. And, since insiders are the leading cause of data breaches, the best way to mitigate the associated risk is by limiting sensitive data access to privileged accounts.

Ask yourself, "How would someone get in our walls?" Coming through the firewall is far from the easiest path. We also find many companies choose to operate under the assumption that a data breach won't happen to them, they're not a target or they don't have anything of value. Misconceptions such as these have guided many companies down the wrong path.

The above are simply a few of the many misconceptions that come with managing the overall cybersecurity of an organization. It's likely not a matter of if; it's a matter of when a data breach will occur.



ATTRIBUTES OF A MATURE CYBERSECURITY PROGRAM

Keeping up with advancements in cybersecurity is a daunting task. The scale at which one can build an effective cybersecurity program is seemingly endless. Whether your company has a $100,000 budget or a $10 million budget, those dollars must be spent wisely among full-time employees (FTEs), security devices and process refinements. Accordingly, sometimes the wisest investment is understanding what you're investing in. What follows is intended to offer guidance as you build and/or mature your current cybersecurity program.

NEEDS VS. NICE TO HAVE

CYBER RISK AREAS	ACTUAL NEEDS VERSUS CYBER RISK AREA "NICE TO HAVES"
CONTROLS	**Need:** User access controls **Nice to Have:** Continuous monitoring and auditing, control mapping to trusted framework(s)
PERIMETER DEFENSE: DEVICES AND TOOLS	**Need:** Modern firewalls, routers, switches **Nice to Have:** Security information and event management (SIEM), log management
SOFTWARE	**Need:** Anti-virus, anti-malware **Nice to Have:** Software-defined perimeter (SDP), mature SDLC and change management

PROGRAM PILLARS

Successful cybersecurity programs mature and grow over time, but all contain a combination of elements such as the following:

- Asset management
- Change and configuration management
- Compliance and governance framework alignment
- Data classification and data loss prevention
- Disaster recovery and business continuity planning
- Employee training and awareness
- Identity and access management
- Physical security
- Perimeter / network security
- Incident response/ management
- Policies and procedures
- Risk identification and assessment
- Supplier/third-party risk management
- Vulnerability management

A PROCESS TO MANAGE CYBERSECURITY RISK

1. Inform leadership on what cybersecurity means to your organization. Educate and provide industry and/or environmental context.
2. Use industry peers to understand what “good” looks like. Achieve progress through choosing a path and driving initiatives forward.
3. Distinguish which data is sensitive. Identify risks, both enterprise-wide and within sensitive domains
4. Calculate cybersecurity risk, which is critical for ongoing management.
5. Develop and roll out program elements (for example, vulnerability management or incident response).
6. Formalize a two-to-three-year strategic cybersecurity plan.
7. Create a system for measurement and reporting.
8. Provide updates on a predetermined frequency to show how things change, measure against milestones, and obtain feedback.

WHAT'S GOOD FOR ME MIGHT NOT BE GOOD FOR YOU

The following case studies are designed to illustrate multiple maturity levels of cyber risk management.

HEALTH CARE PROFILE:

Mid-sized health care entity, domestic US locations only, 1,200 employees, $950 million in annual revenues.

MATURITY LEVEL
7/10

HEALTH CARE PROFILE:
- HIPAA
- HITRUST
- PCI

AUDIT FUNCTION:
- Regional external audit firm
- Internal audit team of three
- Annual audit over IT/Security

SECURITY FUNCTION:
- HIPAA Security Officer
- Internal audit team of three
- Annual audit over IT/Security

CHANGE AGENT:
Fear of HIPAA fines, breach proliferation in media, board of directors.

CURRENT SECURITY PROGRAM FOCUS:
- National Institute of Standard and Technology (NIST)
- Domestic US locations only
- Cybersecurity Framework (CSF) alignment
- Perimeter defense
- Process formalization
- Annual security maturity assessments

BANK PROFILE:

Top 100 US Bank, presence in over half of US, 3,200 employees, over $15 billion in total assets.

MATURITY LEVEL
9/10

IT COMPLIANCE REQUIREMENTS:
- FFIEC
- PCI
- SOX

AUDIT FUNCTION:
"Big 4" external audit firm, internal audit team of 18, recurring audits over IT/Security.

SECURITY FUNCTION:
CISO, Director of Vulnerability Management, three security FTE's.

CHANGE AGENT:
Highly proactive and reputable CISO, comprehensive understanding of security risk.

CURRENT SECURITY PROGRAM FOCUS:
SDP implementation, advanced use of Information Sharing and Analysis Centers (ISACs), regular SIEM refinements.

AUTOMOTIVE PROFILE:

Tier 1 automotive supplier, global presence in 45 countries, 25,000 employees, $9 billion in annual revenues.

MATURITY LEVEL
7/10

IT COMPLIANCE REQUIREMENTS:
- SOX

AUDIT FUNCTION:
"Big 4" external audit firm, internal audit team of six.

SECURITY FUNCTION:
- TCIO
- 3 security FTE's

CURRENT SECURITY PROGRAM FOCUS:
ISO 27001/27002 alignment, vendor risk management program rollout, employee training and awareness.

CHANGE AGENT:
Board of Directors' concerns, customer requests, compliances.

MANUFACTURING PROFILE:

Proprietary manufacturer, presence in multiple US locations, 1,400 employees, $750 million in annual revenues.

MATURITY LEVEL
4/10

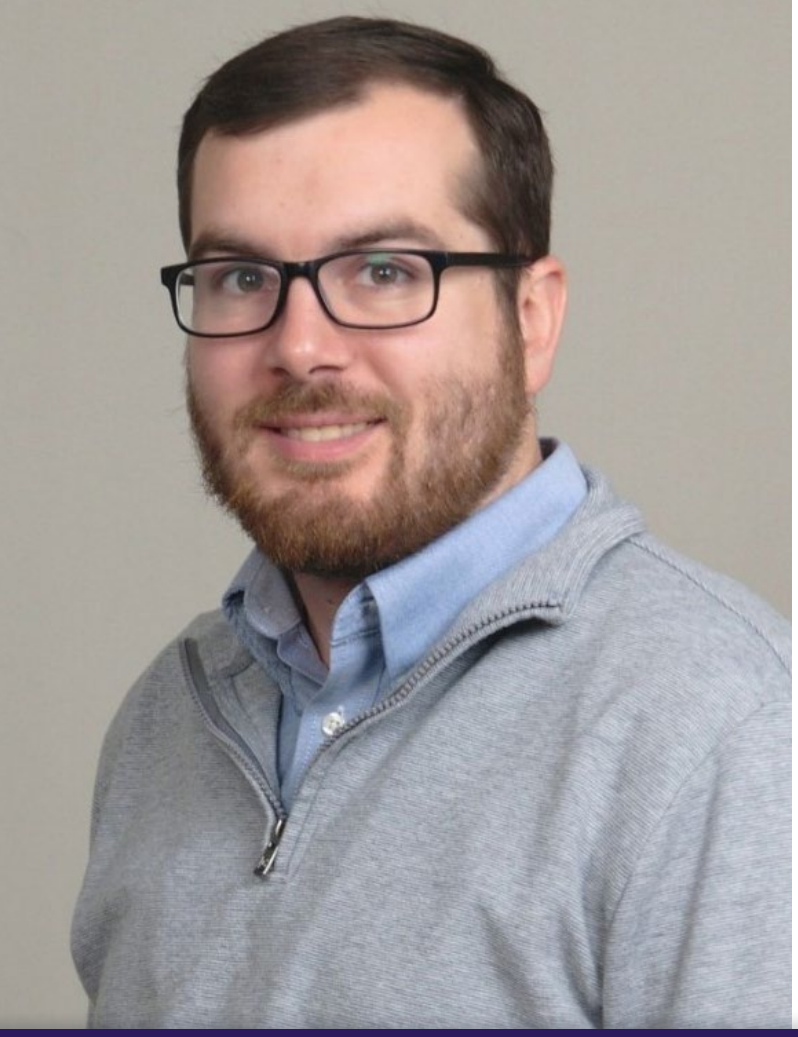
IT COMPLIANCE REQUIREMENTS:
None

AUDIT FUNCTION:
Regional external audit function only, no internal audit staff.

SECURITY FUNCTION:
IT Director, three employees partially dedicated to security

CURRENT SECURITY PROGRAM FOCUS:
Perimeter defense, data classification, partial data loss prevention program.

CHANGE AGENT:
Recognition of intellectual property risk, fear of international duplication/theft.



ABOUT THE AUTHOR

Brandyn Fisher | Senior Manager
Cybersecurity Practice

Brandyn has an extensive background in cybersecurity with more than 10 years of professional experience in the area, an extensive list of security certifications, a Bachelor's in computer security and investigation, and a Master's in cybersecurity and information assurance. Most recently, Brandyn managed a penetration testing and security team as well as led vCISO services for The Mako Group, a cyber risk management firm acquired by Centric Consulting. With a diverse background across multiple industries, Brandon oversaw enterprise projects to bolster the security posture of large financial institutions, hospitals, municipalities and manufacturing entities.

Want to keep your brand reputation and financial impact safe? Our Cybersecurity team can help address your security concerns.

Talk to an expert

((CENTRIC))

ABOUT US

Centric Consulting is an international management consulting firm with unmatched expertise in business transformation, AI strategy, cyber risk management, technology implementation and adoption. Founded in 1999 with a remote workforce, the company has established a reputation for solving its clients' toughest problems, delivering tailored solutions, and bringing in deeply experienced consultants centered on what's best for your business. In every project, you get a trusted advisor averaging over 15 years of experience and the best talent from across the United States and India. Centric deliberately builds teams that can scale up or down quickly based on client needs, industry and desired outcome.

Headquartered in Ohio, with 1,400 employees and 14 locations, Centric has been honored over the years with over 100 awards for its commitment to employees, clients and communities. Most recently, it was recognized by Forbes, for the eighth consecutive year, as one of America's Best Management Consulting Firms.

Visit http://www.centricconsulting.com to learn more.