Does Your Cybersecurity Team Employ the Most In-demand Capabilities?

Here are five key capabilities to consider bringing in-house to build a more resilient team

State-of-the-art cybersecurity is a moving target. New threats appear almost daily, along with new technology to stop them and contain damage. Many organizations focus heavily on deploying the “latest and greatest” security applications and tools. No question, good, current technical tools and infrastructure are essential. But building strong defenses actually depends more on the capabilities of your cybersecurity team. Does it have the most critical current skills needed to protect daily operations and safely enable growth?

It’s a key question not just for CISOs, CSOs, CIOs and others who must hire for hard-to-fill positions, but for the C-suite and board directors as well. Done right, improving in-house security capabilities tied closely to business strategies can foster resilient cyber-defenses that protect against financial and reputational damage while advancing key goals.

The Hot Five

While every organization has unique security needs, these five in-demand capabilities will strengthen and help evolve most cybersecurity teams, regardless of industry, size or risk appetite.

1. Cloud Security

Business services and applications continue moving into the cloud at breakneck speed using IaaS, PaaS and SaaS offerings from Amazon AWS, Microsoft Azure, Google Cloud and others. This rapid adoption demands that your organization develop a cloud security and compliance strategy covering both cloud service providers and end users. Creating proper planning and mitigation policies requires developing mature expertise in cloud architectures, control objects, identification and authorization services, identify governance, and audit considerations. Further, application of ISACA’s COBIT 5 across new requirements, such as GDPR (more below) and PCI, is recommended.

2. AI and Machine Learning

"Smart" algorithms and technologies offer both security opportunity and threat. These powerful tools, such as Artificial Intelligence and Machine Learning apps, can detect and identify attacks and fraud, and ease staff shortages by automating and augmenting security and audit functions. But AI and ML can also *create* new threats that enable anomalous or criminal activity. Organizations need leadership and teams who are expert in managing both benefit and risk, while avoiding related new privacy and regulatory violations. The 2018 Gartner CIO Agenda lists AI as the highest-impact but hardest-to-find skill set.[1] That's doubly true for expertise needed to secure the $46-billion worldwide AI market. Smart companies are making a priority of building capability now.

3. Insider Threats

From hackers using stolen credentials, careless third-party vendors, or negligent or even malicious insiders, user-based attacks remain the biggest IT security threat to organizations, according to the 2017 ISACA State of Cybersecurity research.[2] That makes it more crucial than ever for organizations to field teams that can: build effective insider threat programs; employ the latest best practices; and create frameworks, components, and incident response processes.

4. DevOps Security

More organizations are turning to DevOps to speed the release and improve the quality of software. Closely aligning Development and Operations also introduces new security concerns. However, in recent years a specialty dubbed "DevSecOps" is becoming increasingly vital, helping teams understand and avoid the traps and roadblocks to safely building and scaling apps throughout the Software Development Life Cycle (SDLC).

5. Emerging Technology and Regulations

Internet of Things (IoT). More organizations are also integrating traditionally isolated devices, from IP cameras to HVAC, into business environments. Today's teams must be skilled in understanding and addressing vulnerabilities including data theft, vandalism, remote compromise and other dangers of the new environment.

Blockchain Technology. This current disruptive development is going mainstream, and requires partnerships across the organization to understand and plan for potential security issues resulting from a major rethinking of trusted transactions, from "smart contracts" to proxy votes.

GDPR. Under the strict European Union General Data Protection Regulation (GDPR), released in 2016 with mandatory compliance required this May, cyber risks can

translate into non-compliance. Organizations need the know-how to map GDPR's mandates to vulnerabilities, technical controls, and requirements for overall privacy and security postures.

Building Skills and Capability

Worldwide shortages of experienced, qualified security practitioners have made it especially hard to hire these most-in demand specialties. ISACA's 2017 State of Cybersecurity research also found more than 27 percent of respondents worldwide could not fill open security positions; other new studies put the figure above 50 percent. Skilled talent draws top dollar. It's difficult and time-consuming to vet technical acumen and ability, so companies often end up poaching talent from each other.

To help close the growing supply-demand gap in key areas, more enterprises are building cyber-defense capabilities through training and certification. Some hire talented, fast-learning technology workers and train them for in-demand security skills. Others upskill proven security pros with rigorous programs, including many that provide a wider organizational view of strategy or business practices. ISACA's Certified in the Governance of Enterprise IT (CGEIT) credential, for example, exposes leaders to critical issues around governance and strategic alignment.[3] The CMMI Cybermaturity Platform provides proven pathways to evolve security across people, process and technology into a strategic *business* capability.

Building organizational capability in the most in-demand, most important areas provide the foundation of a new cybersecurity mindset that moves from functional risk-reduction to resilience-driven value creation. Developing the right talent can make or break this crucial transformation.

Cybermaturity.cmmiinstitute.com

Sources

1 – 2018 Gartner CIO Report pdf
https://www.gartner.com/imagesrv/cio-trends/pdf/cio_agenda_2018.pdf

2 – ISACA State of Cybersecurity report
https://cybersecurity.isaca.org/state-of-cybersecurity

3 – ISACA CGEIT credential
https://www.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of-Enterprise-IT/Pages/default.aspx