securitycurrent

MUST-HAVE SKILLS FOR CISOS

by DARREN DEATH

A CISOs Connect Report

TABLE OF CONTENTS

INTRODUCTION

The role of the CISO is highly dynamic and presents great challenges for those who serve in the role for their organizations. There was a time when the information security leader was as a purely technical role, focusing on firewall configurations and password policies. While these aspects of information security are incredibly important, the role has matured to encompass business leadership responsibilities.

Today, the CISO is recognized as a crucial member of the organization's executive team. The role is no longer confined to providing technical support in the information security domain. Rather, the CISO now serves as an enabler to the business functions of the organization.

It is essential that CISOs have the skill set to ensure their organization is hardened against, and has the capability to recover from, a breach.

What skills are critical for the CISO's success?

A survey was conducted of 18 state government CISOs across the United States in 2010 to determine the key success factors related to performing the CISO role. Those key areas include:

1. Communication and presentation skills
2. Policy development and administration
3. Political skills
4. Knowledge about the state government (business / mission)
5. Collaboration and conflict management skills
6. Planning and strategic management skills
7. Supervisory skills
8. Incident management
9. Knowledge of regulation and standards compliance
10. Risk assessment and management

Nine years -- and a lifetime of cybersecurity developments have happened -- since the study was conducted, yet these skills have remained undiminished. In fact, they are as relevant as ever.

1 - Communication and Presentation Skills

Communication and presentation skills are constantly called into play regardless of the role or position of the individual. Whether communicating with executive leadership, a peer team member, an employee, an auditor, or a vendor, it is important to frame the discussion in a way most relevant to the other party. Indeed, framing is everything.

1. When speaking with a peer team member, speak technically and focus on the specific technical implementation that needs to be in place to protect the organization.
2. When working with an employee, turn information security into something that is relevant to their role. Focus on their job function or areas or where they can protect themselves personally to drive home the information security message. `
3. When in discussion with an auditor, the focus should shift to responding to the requirements of the auditor. Accurately and reliably answer their questions without necessarily providing information that may cause confusion.
4. Finally, when meeting with a vendor, ensure that the organization's interests are always a priority and that the requirements related to any contract are fully delivered.

2 - Policy Development and Administration

The CISO is responsible for all enterprise-wide information security policies. In carrying out this duty the CISO is responsible for implementing all legal, regulatory and business requirements. Once those requirements have been delivered, the CISO then develops, promulgates and maintains organizational policy.

When developing your policies, consider the following:

The CISO is responsible for ensuring that policy is developed from a project management perspective. This includes resource management and allocation to ensure that the full policy deck is developed and is socialized with all required organizational team members.

Policy that is developed and set on a shelf is useful to no one. Therefore, the CISO is responsible for ensuring that new policy is communicated appropriately throughout the organization.

Finally, the CISO is responsible for the continued maintenance of policy. Periodically the CISO will review the information security policy for the organization ensuring that the policy still meets legal, regulatory and business requirements.

3 - Political Skills

Being able to interact effectively within the organization is critical to the success of the enterprise information security program, therefore making political skills an important CISO skill.

The CISO should understand the needs and concerns of the executive team (as they relate to the mission of the business) and then present the information security program as a response to these needs.

To peer team members and users, the CISO should communicate that information security findings are not accusatory or punitive, and that policy is not meant to hinder them from doing their jobs. Rather, the security policy exists to help everyone perform their jobs better and more securely.

The CISO should implement a rigorous organizational change management processes to ensure highly effective communication that presents how information security changes are designed to protect the organization and ultimately the jobs of all employees.

4 - Knowledge and Understanding of the Business and its Mission

The most important thing that CISOs can do is integrate themselves appropriately with the mission of the organization, but it can also be the most challenging. Without this deep integration, it difficult to establish mission value for any new cyber initiatives.

It has been identified in academic literature that there is a perceived high rate of failure related to the implementation of Information Technology projects even when the project is 100% compliant with its requirements. An effective mechanism to overcome this problem is ensuring that the technology program is well integrated with the mission so that new technical projects are focused on delivering benefits to the mission versus simply delivering functioning IT systems (Doherty, N. F., Ashurst, C., & Peppard, J. 2012). By addressing this gap, the IT program is establishing itself as a business enabler rather than simply focusing on the technology it is delivering.

Research has discovered that Information Technology projects are immediately more successful when top-level business / mission senior executives are "actively" supporting an important technology project (Karanja, E. 2017). It is incumbent upon the CISO to work with mission leaders ensuring that new security projects have the necessary mission value that will ultimately contribute to improved organizational resiliency and productivity. Once this relationship has been established and appropriately communicated to the organization, the CISO should seek out mission leaders to champion and drive new security projects and support the ongoing security activities of the CISO's organization. In doing so, the security project becomes a mission activity rather than a security activity where the organization's senior leadership is supporting new and important security changes that will support the organization's continued success.

5 - Collaboration and Conflict Management Skills

A CISO's job is no longer confined to staying in front of the computer, on the lookout for security breaches. The role is now called upon to collaborate with members of the organization's mission team, peer technologists and end-users.

When collaborating with the mission team, the CISO now works to solve an issue that is related to the successful operation of the organization rather than simply serving to provide a solution for an individual's job function. Together with the mission team, a secure solution is developed while also ensuring that organizational productivity remain high.

When working with peer technologists, the CISO must ensure that security requirements are well explained, and that effective guidance is provided. This ensures that security controls are properly implemented the first time, minimizing any rework.

When working with end users it is important to develop the needed training and guidance that drive the adoption of information security practices by the organization's end user community.

6 - Planning and Strategic Management Skills

A CISO is a manager; hence, planning and strategic management come with the territory. Effective information security program management requires strong planning and strategic management skills to manage the incredible pace of change in the technology industry and the way that organizations are using new technologies.

How should CISOs engage their organizations to achieve strong support for the information security program?

Step One

Information security activities must align with and support the organization's strategic plan. When the leadership supports and sponsors cybersecurity activities, there will be greater adoption of such practices across the organization (Karanja, E., 2017).

Step Two

The CISO should be abreast of all technology projects across the organization, so that the cybersecurity program can be integrated in them at the outset, instead of being bolted toward the end or not being included at all. This would also significantly reduce the information security engineering costs of reworking the project.

Step Three

The CISO needs to anticipate changes in cybersecurity while managing the information security program and ensuring defensive, monitoring and incident response technologies and processes are in place. Periodic assessment should take place including a review of people, policy, processes and technology to ensure that the program continues to deliver envisioned results.

7 - Supervisory Skills

A team of effective information security professionals is needed for any robust information security program. It is not just one person -- the CISO -- but an able group or team that works well together. Mentoring and the ability to prioritize and communicate priorities to the team are key and important to the execution of the CISO role.

Mentoring, and mentoring well, is critical in the cybersecurity field. As information security can be a very generalist profession, the need to share information with peers is extremely important. Working with the team to develop their skills leads to a much more engaged team, resulting in a more effective and knowledgeable information security program.

Likewise, setting and communicating priorities is critical. As an information security program can be called on to meet new challenges daily, prioritization is a critical skill for the CISO. The CISO needs to balance the needs of the business (IT organization, security projects and incidents) while making sure the team remains fully engaged and does not fatigue from constant change.

8 - Incident Management

It is well recognized that a well-resourced adversary will eventually be able to breach the defenses of even a well-defended organization. Thus, establishing an incident response program that can detect intrusions on the network and immediately work to clean and recover from those intrusions is critical (Zafar et al 2016).

The several stages of an effective incident management plan include:

Preparation. The activities related to establishing and executing a well thought out and effective incident response program.

Identification. The activity of intrusion discovery.

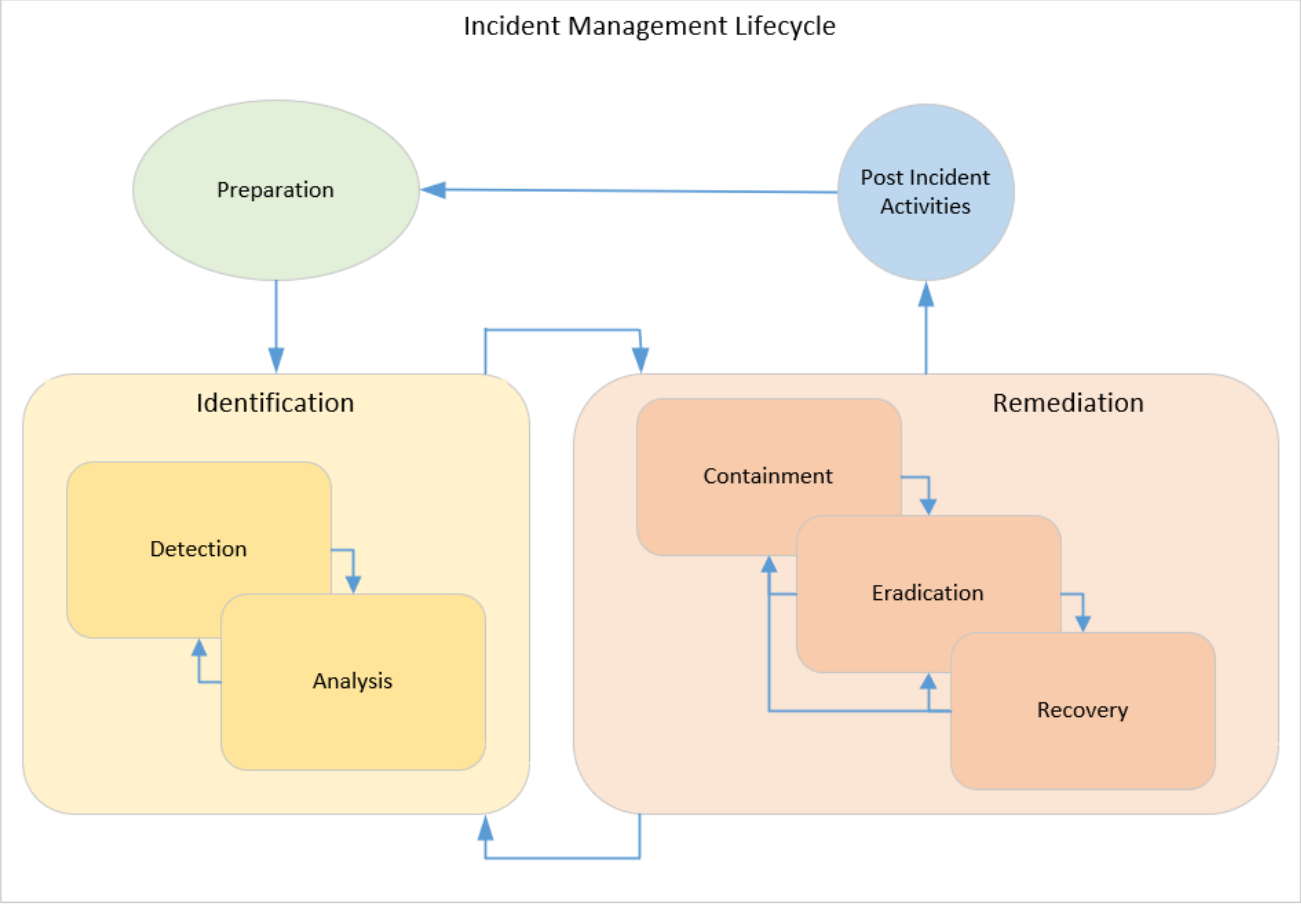
- Detection: Combination of technical tools and human resources used to detect the presence of a malicious actor.
- Analysis: Combination of technical tools and human resources to validate the presence of a malicious actor.

Remediation. The activity related to intrusion eradication.

- Containment: Ensuring that the malicious actor cannot infect any new information systems.
- Recovery: Eradicating the malicious actor from the information system.
- Mitigation: Ensuring that the information system is configured so that it can no longer be exploited.

Post-Incident Activity. Lessons learned that are used to improve the process as a continuous process.

These stages, when implemented correctly, establish an incident management life cycle that ensures effective planning, management, and continuous improvement as outlined in the below drawing (Death 2017).



9 - Knowledge of Regulation and Compliance with Standards

The CISO must be an authority in the regulation, standards and compliance requirements applicable to the organization. This knowledge is important so that the CISO can tailor their expertise to meet the specific needs of their organization, leading to the development of compliant information security policies, processes, procedures standards and guidance.

If the information security program does not meet the requirements of auditors and regulators, there will be severe penalties imposed on the organization no matter how effectively the program protects it from external threats.

10 - Risk Assessment and Management

Risk assessment and management establish key processes used for communication between the organization's executive leadership and the CISO.

Risk ownership is always a C-Suite/Board Level/Executive Leadership issue, so establishing a business-level line of communication between executive leadership and the information security program is vital to establishing a risk management program. The risk management program and its outputs (like the risk register) must always be aligned with the business to be effective.

As the CISO constructs and operates the organization's risk management program, they will:

- Discover the organization's valuable data
- Select, implement and assess appropriate security controls
- Authorize information systems to operate
- Identify organizational threats and vulnerabilities
- Estimate likelihood and impact of organizational disruption

The risk management program feeds other aspects of the organization's information security program such as security architecture and incident response.

For security architecture, it clearly defines the risk appetite of an organization's executives and establishes the necessary controls to implement while guiding a new information system through the system development life cycle. It also establishes the justification for information security related decisions to both business managers and IT professionals.

For incident response, the risk management program allows the CISO to effectively triage new incidents and provides the correct context to establish network zones and enclaves. With this information in hand, the information security and IT teams can more easily determine which issues need immediate review (all hands-on deck) and which issues can be scheduled for remediation.

CONCLUSION

Cybersecurity is a dynamic industry and the threat landscape changes quickly. CISOs, too, come in all shapes and sizes.

The key success factors related to performing the CISO role may be different depending on the CISO's background and personality. The specific success factors may also be determined by the needs of their respective organizations and the prevailing security culture within them.

Discussed above are a timeless set of skills. These skills are necessary to effectively lead the integration of technology with the business and mission of the organization, and aligning the security program with the needs, targets and priorities of the people within.

REFERENCES

Goodyear, M., Goerdel, H., Portillo, S. Williams, L. (2010). Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers. Retrieved from: https://its.ny.gov/sites/default/files/documents/cybersecurity-management-in-the-states-ibm-kansas-u-report-may-2010.pdf

Doherty, N. F., Ashurst, C., & Peppard, J. (2012). Factors affecting the successful realisation of benefits from systems development projects: Findings from three case studies. Journal of Information Technology, 27(1), 1-16. doi: http://dx.doi.org.library.capella.edu/10.1057/jit.2011.8

Karanja, E. (2017). The role of the chief information security officer in the management of IT security. Information and Computer Security, 25(3), 300-329. doi: 10.1108/ICS-02-2016-0013

Zafar, H., Ko, M. S., & Osei-bryson, K. (2016). The value of the CIO in the top management team on performance in the case of information security breaches. Information Systems Frontiers, 18(6), 1205-1215. doi: http://dx.doi.org.library.capella.edu/10.1007/s10796-015-9562-5

Death, D. (2017). Information security handbook: Develop a threat model and incident response strategy to build a strong information security framework. Birmingham, UK: Packt Publishing.

ABOUT THE AUTHOR

Darren Death

Vice President of Information Security, Chief Information Security Officer at ASRC Federal

Darren Death is ASRC Federal's Chief Information Security Officer. Death is responsible for managing the enterprise cyber security program across a $3-billion portfolio of business sectors including financial services, government contracting and construction.

A proven technology leader with over 20 years of experience deploying enterprise systems for large private and public organizations, Death has led, designed, and implemented large-scale, organizational wide enterprise IT systems with far reaching impact. Prior to joining ASRC Federal, while at the Department of Justice, Death was responsible for the creation of a nationwide enterprise processing capability across US Attorney's, Marshalls Service, and Alcohol Tobacco and Fire Arms divisions. At the Library of Congress, Death was responsible for all emerging technologies as it related to information security.

Death holds a master's degree in Cybersecurity and Information Assurance and is currently working toward his Doctorate in Information Technology - Information Assurance and Cybersecurity. Death currently serves on the EC-Council Global Advisory Board for TVM (Threat and Vulnerability Management) and serves as the InfraGard Maryland – Cyber Threat Special Interest Group Chief and American Council for Technology / Industry Advisory Council (ACT-IAC) – Cyber Security Community of Interest Program Chair.

Security Current improves the way security, privacy and risk executives share information and collaborate to protect their organizations and their data. Security Current also runs CISOs Connect, a knowledge-sharing platform exclusively for CISOs. Its CISO-authored and peer-driven proprietary content and events provide insight, actionable advice and analysis giving executives the latest information to make knowledgeable decisions.