Building a Risk-Based Information Security Culture

By Donald A. McKeown – ISSA member, New England Chapter

An effective security culture will be risk-based, requiring an organizational structure with visibility and influence, moving beyond ad hoc and complicance-based, and understanding the business's risk appetite. The goal of this article is to offer guidance about how and why to build a risk-based security culture.

Abstract

An often-overlooked foundation of an effective information security program is culture. An effective security culture will be risk-based. To build such a program, the organization needs to set information security leadership appropriately in the organizational structure to have the required visibility and influence to shape culture. Leadership needs to create a road map that moves the organization from ad hoc and compliance-based cultures to one that's risk-based. Management needs to understand the business's risk appetite, codify it as policy, and drive behavior consistent with this policy throughout the organization. In addition, the culture should focus on learning from incidents rather than blaming.

Companies build strong organizational cultures to help ensure business success. Organizational culture "defines the proper way to behave within the organization. This culture consists of shared beliefs and values established by leaders and then communicated and reinforced through various methods, ultimately shaping employee perceptions, behaviors, and understanding."[1] For example, companies that establish a culture that enhances employee engagement tend to outperform in the long-term companies with lower engagement.[2] Moreover, there is evidence that organizational cultures that promote employee engagement result in better business performance, not that better business performance results in a better culture.[3] In other words, organizations should establish a strong culture first to optimize business performance.

Given that successful businesses create organizational cultures that drive business performance, one might expect that companies also create cultures to protect their information assets. However, this is typically not the case, as culture is often not considered as part of an information security program. Moreover, given that security is a relatively immature discipline, security programs tend to be guided more by beliefs and values rather than standards and data. Therefore, transforming and improving security programs is much about reshaping the security culture. The goal of this article is to offer guidance about how and why to build a risk-based security culture, one with a consistent, shared belief that in-

1 "Understanding and Developing Organizational Culture," Society for Human Resource Management (August 13, 2018) - https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/understandinganddevelopingorganizationalculture.aspx.

2 David Brown, Veronica Melian, Marc Solow, Sonny Chheng, Kathy Parker, "Culture and Engagement: The Naked Organization," Deloitte (February 27, 2015) - https://www2.deloitte.com/insights/us/en/focus/human-capital-trends/2015/employee-engagement-culture-human-capital-trends-2015.html.

3 Dan Pontefract, "If Culture Comes First, Performance Will Follow," Forbes (May 25, 2017) - https://www.forbes.com/sites/danpontefract/2017/05/25/if-culture-comes-first-performance-will-follow/#4b41d3096e62.

formation security should be proactive rather than reactive, that risks can be openly discussed, and that security is a process that needs to continually be monitored, evaluated, and improved. In such cultures, staff widely understand and believe in leadership's stated risk appetite for the organization.

Effective security programs

People, process, and technology is the foundation of an effective security program. Culture is part of the "people" foundation. Yet, many companies prioritize technology first, followed by process, and then people[4] in their approaches to mitigating information security risk. For example, if a company is worried about sensitive data leaking out, often the first response is to implement a data leakage prevention (DLP) solution. Responses of this type are fueled in part by the security technology industry that preys on fear, uncertainty, and doubt to convince many that buying a technology solution will address the problem.

Compliance obligations also drive a technology-centric approach. For example, PCI A3.2.6 states "Implement mechanisms for detecting and preventing cleartext PAN from leaving the CDE via an unauthorized channel, method, or process, including generation of audit logs and alerts."[5] DLP will check that box.

While technology solutions are a crucial part of addressing the rapidly changing threat environment in a scalable, efficient manner, they are not enough. Another element is the maturity of the processes associated with the technology. Tools can't merely be "bolted on" a network to address risk. Once a tool is implemented, there need to be documented organizational processes to regularly tune it, updated it, and respond to the alerts it generates. Furthermore, these processes need to be measured, continually improved, and governed.

Once technological solutions are established with some degree of process maturity, organizations might address the people element of the security program. In the DLP example above, a company might have staff learn on the job, or perhaps invest in formal training. At the organizational level, companies frequently have annual security compliance training that consists of relatively brief online sessions followed by quizzes.

However, building an effective security program needs to go beyond technology, technology-specific processes, and "check the box" annual compliance training. First, the Chief Information Security Officer (CISO) needs to be placed properly within the organizational structure. Then, the CISO should create a road map towards a risk-based security culture that aims to progress beyond ad hoc processes and compliance-based, control-oriented security programs to a program that is proactive, uses multiple layers of defense, and regularly evaluates new defenses. Also, such a program will monitor the threat environment and collaborate with peers regarding defense. The specifics of the security strategy will depend on senior management's risk appetite. Once senior leadership decides on a security strategy, it will codify it in policy and seek behavior consistent with this strategy throughout the organization.

Place CISO in organization appropriately

Organizations that are committed to security need to position the Chief Information Security Officer appropriately in

4 Lance Hayden, *People-Centric Security: Transforming Your Enterprise Security Culture*, McGraw-Hill Education (2015).

5 "Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures, Version 3.2.1," Payment Card Industry (PCI) Security Standards Council (May 2018) - https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf.

the organizational structure. Ideally, the CISO should report directly to the Chief Executive Officer. If the CISO reports elsewhere, then leadership needs to understand the related trade-offs.

The CISO needs to be able to advocate for an appropriate budget to mitigate risk across the entire organization. If the CISO is buried in an organization below the CEO such as the Chief Information Officer (CIO), it's more challenging to achieve organization-wide visibility and context (an even worse scenario is reporting into Legal). To be truly effective, the CISO needs to be able to advise not only on, say, the CIO's projects, but projects that arise anywhere in the organization.

In addition, the CISO needs to be able to advise on projects early in conception to ensure that security is baked in from the beginning. The later flaws are discovered in the project cycle, the more expensive they are to fix. Another risk of the CISO reporting to the CIO is that security budget could be slashed in favor of projects more central to the CIO's charter.

Furthermore, this reporting relationship is a conflict of interest because the CIO could be biased to ignore or downplay security vulnerabilities in the systems for which he or she is accountable and may not want to allocate time for security reviews and fixes if it may delay a project implementation or take time from other projects. A CISO at the same organizational level as the CIO can advocate on equal footing for security.

Finally, the CISO reporting to the CIO could violate the segregation of duties principle.[6] For example, the CIO team is typically responsible for adding, modifying, and deleting user accounts in systems such as Active Directory. The CISO function is often charged with monitoring the user account life cycle via access control reviews and responding to alerts indicating potential malicious user account activity. These two functions should be independent to avoid misuse and unintentional changes of user accounts; separating the CIO and CISO organizations will achieve this. This may not be practical for smaller organizations, so compensating controls such as multiple authorizations for account changes could be implemented.

A high-profile example of an organizational structure increasing risk for a company is the Equifax breach.[7] It's well understood that attackers exploited a known, unpatched Apache Struts vulnerability. What's not gotten enough attention[8] was that, according to the Congressional report on the breach, the root cause of the vulnerability not being fixed was organizational: "The functional result of the CIO/CSO structure meant IT operational and security responsibilities were split, creating an accountability gap."[9] When the breach occurred, the CSO was within the Legal organization. As of December 2018, the CSO is now called the CISO and reports to the CEO.

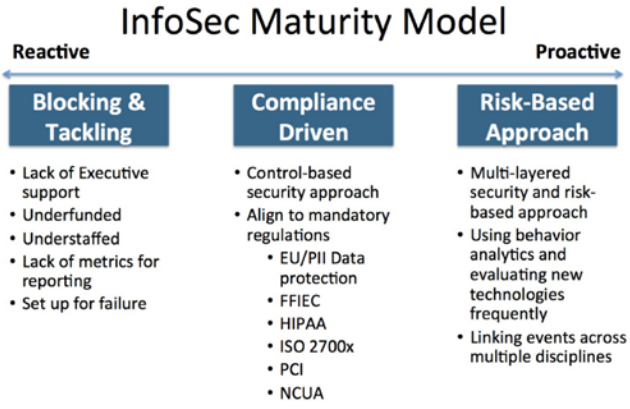

Figure 1 – The Blue Lava information security maturity model

The good news is that organizations are improving their organizational structures. In 2018, Accenture conducted a survey of companies with $1 billion or more in revenue regarding security ownership. The CEO or board of directors directed cybersecurity in two-thirds of the companies; CIOs ran security in about the remaining third—a decrease of six percent since 2017.[10] This survey did not address companies with less than $1 billion in revenue, but it's more likely that companies in this group bury security within technology or other organizations.

Once an organization has security placed appropriately in the organizational structure, it then needs to decide what kind of security culture it wants to build. Without an appropriate culture, security will be limited in its effectiveness.

Security should adopt a risk-based culture

The most effective security organizations will build a risk-based program. The maturity of a security program reflects the organization's shared beliefs and values about security, so evolving to a risk-based program is fundamentally a cultural shift, which must start with leadership buying into such a change and creating a path to get there. The Blue Lava maturity model describes such a road map in three stages (see figure 1).[11] Please note that this maturity model also has a five-point process maturity scale I will not be describing.

The least mature stage is ad hoc. This stage is based on an organizational culture that does not value security. In this stage, security lacks executive support, lacks enough funding, and is understaffed. It primarily reacts to incidents and re-

6 Robert Putrus, "The Role of the CISO and Digital Security Landscape," ISACA Journal (Volume 2, 2019) - https://www.isaca.org/Journal/archives/2019/Volume-2/Pages/the-role-of-the-ciso-and-the-digital-security-landscape.aspx.

7 Brian Krebs, "A Chief Security Concern for Executive Teams," Krebs on Security (December 2018) - https://krebsonsecurity.com/2018/12/a-chief-security-concern-for-executive-teams/.

8 Lance Spitzner, "The Congressional Report on Equifax Hack," SANS (December 17, 2018) - https://www.sans.org/security-awareness-training/blog/just-released-congressional-report-equifax-hack.

9 "U.S. House of Representatives, Committee on Oversight and Government Reform-The Equifax Data Breach," Majority Staff Report, 115th Congress, (December 2018) - https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf.

10 Kate Fazzini, "Companies Unleash CISOs from Ties to Tech Chiefs," Wall Street Journal, (April 24, 2018) - https://www.wsj.com/articles/companies-cut-ciso-reporting-ties-with-technology-1524515201.

11 Richard Roberts, "Measuring Cybersecurity Readiness: The Cybersecurity Maturity Model," NCHICA Cybersecurity Thought Leader Forum - https://nchica.org/wp-content/uploads/2016/10/Roberts.pdf.

quests. There are few if any formal security processes, reporting metrics, or overarching guidance in security. This stage is the least effective, as there is no authoritative guidance or measurement of efforts—a program that's "set up for failure."

The next stage of maturity is compliance driven. This stage is based on a culture that believes passing a compliance audit means it's secure. In this stage, security efforts are control based and driven primarily toward satisfying compliance requirements. One advantage of this stage over ad hoc is that the program is based on authoritative standards. The security culture in this stage is characterized as believing that when compliance requirements are met, the company is secure. While compliance is needed for satisfying legal and regulatory requirements and is responsible for improving security significantly across the industry, it is not enough in this world of rapidly evolving advanced threats.

We Are the Front Lines – Protecting Yourself Protects the Organization

Continued from page 9

victim's front door once the credentials are known. However, most organizations have built a second door to go through (second factor of authentication: what you have), that must be breached to get into the victim's account. Thanks to human error, an attacker can successfully pass through both doors.

Two-factor authentication (2FA) – A false sense of security

Two-factor authentication is the next logical step for securing the front door. According to the Anti-Phishing Working Group,[2] between October 2015 and March 2016 the use of 2FA surged by 250 percent. Merely implementing 2FA is not enough. It requires user training and awareness to be effective. Both the organization and the employee need to understand their roles in properly using 2FA.

Once an organization implements 2FA on its network and applications, it can fall into a false sense of security that user credentials are safe. While there are various technical methods to circumvent 2FA, one popular method is to rely on the unsuspecting individual to let the attacker into the second door. This may seem far-fetched, but I have actually seen this happen in the work place in the following scenario.

> **This actually happened:** A popular attack vector is to capture the individual's credentials and log into the victim's web-based email account. Once the attacker uses the individual's credentials to log in, he will be faced with a second screen or dialog requesting a second factor of authentication. He appropriately requests a push for approval, which typically goes to the legitimate user's mobile phone. The user, without paying attention, answers and hits the *approve* button. The attacker now has access to the individual's email.

Treasure trove

Once the attacker is in the individual's email (he's now an intruder), the intruder conducts a quick search of the inbox and folders for any potentially sensitive data. It is no surprise, especially to the intruder, that the user stores a significant amount of personal and professional data in work email (e.g., spreadsheet with personal and work passwords, word document with personal and/or work credit card numbers, etc). With the aforementioned scenario, the forensics analysis team discovered that the individual had approximately five years of email in various folders, including the deleted folder (human error strikes again: user didn't realize that deleting an email didn't really wipe the email out of the system). The first thing the intruder did was to conduct a search on keywords such as "credit card" and "account" to find sensitive data in the body of the email or in the attachments. As it turns out, the individual had sensitive data in various spreadsheet attachments.

Protecting ourselves

It's critical that individuals protect themselves at home and in the work place. These two environments are virtually linked in the cyber attacker's eye, and he continues to exploit this weakness in an organization's cybersecurity defense posture. The first line of defense in an organization's cybersecurity strategy should be the individual. That first line must be strengthened to mitigate the risks of a successful attack via social engineering and phishing on the organization's employees. The organization must invest in cybersecurity as a holistic program—people, processes, and technology—cradle-to-grave.

Implementing a holistic cybersecurity program with a continuous cybersecurity awareness program (not to be confused with annual security training) will go a long way in protecting the front lines against social engineering and phishing. Each individual must understand the critical role that he or she plays in protecting the confidentiality, integrity, and availability of the organization's data. Ensuring that we are protecting ourselves is not easy. The cyber criminal is resourceful and relies on human error to gain access to a treasure trove of sensitive data that individuals fail to adequately protect from unauthorized access.

About the Author

Tony Buenger, CCISO, CISSP, CISM, CGEIT, assumed the role of CISO for Augusta University in 2018. Tony served as an Associate Professor for the National Defense University. He holds a Master of Military Operational Art and Science and Master of Arts, Space Systems Management. He can be reached at tonybuenger@yahoo.com.

2 Bradley Barth, "APWG Report: Phishing Surges by 250 percent in Q1 2016," SC Magazine (May 25, 20160 – https://www.scmagazine.com/home/security-news/apwg-report-phishing-surges-by-250-percent-in-q1-2016/.

Two high-profile examples that demonstrate compliance alone is insufficient are Target and Heartland Payment Systems, which were both certified PCI-DSS compliant yet suffered massive breaches. More generally, evidence suggests that breached companies do not generally maintain their controls after the initial certification assessment. One analysis, citing Verizon's PCI DSS Compliance Report, noted that "only 29 percent of companies are compliant a year after validation."[12] Furthermore, this analysis cited the Verizon 2015 PCI Compliance Report: "Of all the companies investigated by our forensics team over the last ten years following a breach, not one was found to have been fully PCI DSS compliant at the time of the breach."

The analysis also argued that there is a misconception that PCI DSS-certified companies are "secure or hacker-proof." PCI DSS addressed the most prevalent threats when it was written. The most recent version (3.2.1) was published in May 2018; the previous version (3.2) was published in April 2016. In the two years between 3.2 and 3.2.1, the threat landscape changed significantly, so if an organization remained compliant with version 3.2 for two years, the company's controls were falling behind the rapidly shifting threat landscape during that time. Moreover, the analysis noted that PCI DSS could not account for all threat scenarios. Ultimately, a company is responsible for protecting its cardholder data, and it can't do so by only passing periodic compliance audits. It must adopt a continuous risk-based defensive posture to safeguard its PCI assets adequately.

12 Christian Moldes, "Compliant but Not Secure: Why PCI-Certified Companies Are Being Breached," Journal of Cyber Security and Information System, Volume 6, Number 1 (05/09/2018) - https://www.csiac.org/journal-article/compliant-but-not-secure-why-pci-certified-companies-are-being-breached/.

Furthermore, compliance obligations apply only to specific environments. For example, PCI applies only to segregated environments that store, process, or transmit credit card data. Even ISO 27001, a process-oriented standard that can form the basis for an effective program, must be scoped to defined areas. Attacks can occur anywhere in a company's systems, or its third-party partners. Attackers can move laterally from less secure areas to attack more protected areas. Also, personnel throughout the organization can make mistakes that increase the risk of attack. Compliance cannot be the basis of an effective, comprehensive, organization-wide security program.

Regardless, it's difficult if not impossible to build a risk-based program without the basis of a strong set of fundamental controls. Assuming the organization has no mandatory compliance obligations such as PCI or HIPAA, it needs a framework on which to build its controls. ISO 27001 is a fine, non-mandatory standard that's often suggested, but for companies still in the ad hoc stage, it can be overwhelming. An excellent starting place is the Center for Internet Security (CIS) Controls.[13] It's prioritized, IT staff will likely understand the controls easily, and there's a measurement companion that offers metrics. Moreover, the controls map to ISO 27001, so it will put an organization on the ISO 27001 path.

If the company has achieved mandatory compliance requirements, it can be difficult to persuade leadership to commit to building a risk-based culture. One possible reason that early in the building of a company, leadership may have believed it needed to focus almost exclusively on building product features and invest the bare minimum to achieve compliance standards. This belief could persist as the company matures

13 Center for Internet Security (CIS) Controls - https://www.cisecurity.org/controls/.

unless there's a compelling reason such as an incident to change.

Regardless of the reason, education about the threat environment using data from credible sources such as the Verizon Data Breach Investigations Report (DBIR) as it relates to the organization combined with internal data such as incident statistics can help. Regular briefings about the current threat environment, how it could affect the company in business terms, and recommendations for action are of value. Note that it's critical not to put a stop to business operations over every emerging threat or to attempt to use FUD to drive change. Thoughtful, data-based reporting regarding threats and the potential risk they pose to the business will help security become a trusted advisor to the business. Management has the prerogative to knowingly accept risk.

Successful, well designed penetration tests or red team exercise results can also help shift attitudes, if the results are contextualized properly. Yes, it's critical to address the specific findings of the report, but it's important to know that good red team/penetration testers can almost always find a way to compromise an organization, as can attackers. Building a risk-based based culture will help prevent such attacks and detect them earlier when they inevitably occur. Another lesson is that organizations need to build the capability to recover from damage as a result of compromises.

Regardless of whether a company is in the ad hoc stage or compliance stage, customers needing assurance regarding the organization's security can drive significant change. Business's often pursue a Service Organization Control 2 (SOC 2) attestation to fulfill that need. A SOC 2 is not strongly prescriptive like PCI. Controls need to align with certain criteria, so the organization has latitude in designing them. This is a fantastic opportunity for security leadership to architect strong controls and to partner with leadership to build a risk-based security culture. For example, a security awareness program, a control typically found in SOC 2s, could be designed that requires senior leadership to speak quarterly to employees about the importance of security, to articulate their expectations, and to recognize teams or individuals that exemplify strong security.

A risk-based approach to security, the most mature stage of the Blue Lava maturity model is based on a culture that values proactive security and understands that security is an ongoing process that must be continuously improved, based on changes in threats and technology. Senior leadership needs to set expectations that it wants such a culture and program. Typically, such programs use defense in depth, correlate events across the organization, deploy behavioral analytics to detect events indicating malicious activity, and periodically evaluate new security technologies. I would also argue that mature organizations will possess the capability to recover quickly and effectively from damage caused by inevitable compromises.

Achieving such a program is a high bar for many organizations. Therefore, it's critical to prioritize and set goals that make sense for the organization. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)[14] provides valuable guidance. The framework implementation tiers "provide context on how an organization views cybersecurity risk and the processes in place to manage that risk." There are four tiers: partial, risk-informed, repeatable, and adaptive (figure 2). The CSF makes it clear that "tiers do not represent maturity levels. Progression to higher tiers is encouraged when such a change would reduce cybersecurity risk and be cost-effective."

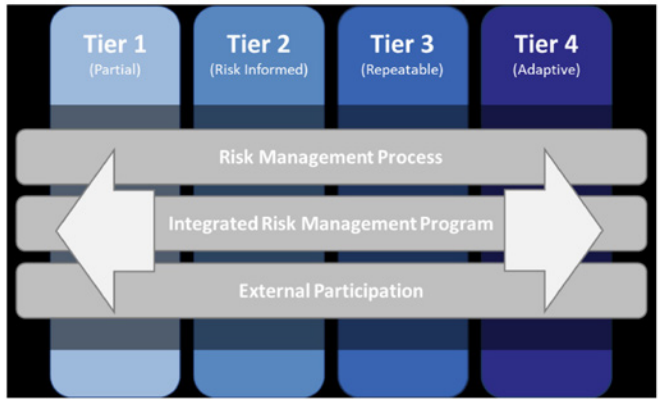

Figure 2 – NIST CSF implementation tiers[15]

Within each tier, there are three domains. The process related to each domain becomes more formal and rigorous as it moves from partial to adaptive. The three domains are *risk management process, integrated risk management program,* and *external participation.* I refer you to the original text for details, but there are some important takeaways.

First, a risk management process and program are not optional. Using an authoritative standard such as the CSF can help persuade leadership as to the necessity of a risk program. Ad hoc or compliance-driven organizations must develop a road map to building risk processes and programs. The only question is which tier makes the most sense. As noted, the NIST CSF encourages organizations to target higher tiers when the risk and cost analysis justifies it. Most will do this in a qualitative manner, but the most persuasive, rigorous approach is using a proper quantitative approach. For more information, I suggest starting with Douglas W. Hubbard's *How to Measure Anything in Cybersecurity Risk*[16] and Jack Freund's *Measuring and Managing Information Risk: A FAIR Approach.*[17]

The external participation domain of the NIST CSF also complements Blue Lava's model. This domain refers to learning from and sharing with others information about threat intelligence, best practices, and new technologies. Given the

14 "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.1, National Institute of Standards and Technology (NIST) (April 16, 2018) - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

15 NIST, "An Introduction to the Components of the Framework," NIST – https://www.nist.gov/cyberframework/online-learning/components-framework.

16 Douglas W. Hubbard, Richard Seiersen, *How to Measure Anything in Cybersecurity Risk*, Wiley, (2016).

17 Jack Freund, Jack Jones, *Measuring and Managing Information Risk: A FAIR Approach*, Butterworth-Heinemann, (2014).

rapidly shifting threat and technological environment, it's critical to monitor and respond to emerging threats. This element also refers to awareness of cyber supply chain risks. Attacks against supply chains are increasing,[18] and the NIST CSF greatly expanded its related guidance in the latest version (1.1).

If policies are relatively strict, but the business needs a more aggressive risk posture to achieve its goals, then staff are not likely to comply with the policy.

Ad hoc and compliance cultures can be deeply ingrained and difficult to change. Unfortunately, it often takes a serious incident to catalyze a cultural shift. The better approach is to educate leaders about the weaknesses in these cultures. Once leadership understands these weaknesses, they can use guidance from the ISACA RiskIT Framework to build a risk culture, which is the foundation of an effective information security program.

The ISACA RiskIT framework

ISACA's RiskIT framework,[19] which is focused on balancing risk and value, provides explicit guidance for building a risk-aware culture. The three major categories of RiskIT processes are *risk governance, risk evaluation,* and *risk response*. One of the key activities of risk governance is RG 1.5 - "Promote IT risk-aware culture." See figure 3 for the elements of risk culture.

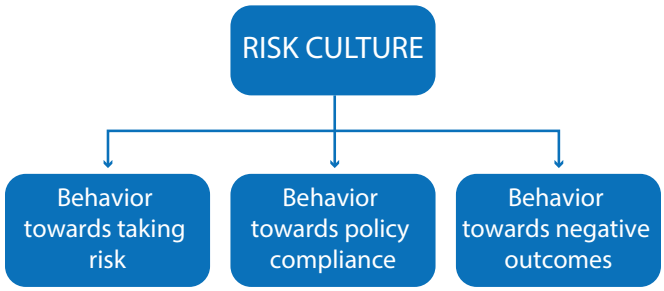

Figure 3 - Elements of risk culture, per RiskIT framework

In a risk-aware culture, executive leadership will formalize their appetite for risk as policy. Risk appetite will be related to the previously discussed NIST CSF implementation tiers. A lower risk appetite requires a higher, more rigorous implementation tier. If policies are relatively strict, but the business needs a more aggressive risk posture to achieve its goals, then staff are not likely to comply with the policy. Business leadership should view security policy as an opportunity to communicate how they want the business to operate.

Once risk appetite is expressed in policy, it must be regularly communicated across the organization. All staff need to understand it, buy into it, and consistently act on it. When situations arise that expose the organization to risk such as incidents, penetration test findings, or threat modeling that indicates design flaws, a risk-aware culture facilitates open discussion of these issues. Such dialog is more likely when management consistently communicates their position on risks, encourages open communication regarding risk, and models it in their own behavior.

Subgroups within the organization that don't buy into management's risk appetite can cause unanticipated risk. If the organization needs to grow rapidly, and it needs to take on a high amount of risk to achieve its goals, then all teams need to buy into this direction and act on it. Management may want to allocate fewer resources towards building security controls in a product than security wants so that it can deploy more resources toward building product features. This conflict could drive management to avoid consulting with Information Security, which could result in overly risky decisions.

If an organization has a low or moderate appetite for risk, departments or subcultures that believe it should take on higher risk, perhaps to innovate or get things done more quickly, might circumvent security measures or avoid consultations with Information Security to achieve their aims and put their organization at undesired risk. For more information about how to build consistent security within an organization, please see Lance Hayden's *People-Centric Security: Transforming Your Enterprise Culture.*

Organizations will experience adverse outcomes such as incidents or missed opportunities. A risk-aware culture, instead of blaming individuals or groups, will use these situations as learning opportunities. One way is to conduct a root cause

18 Dan Goodin, "Two New Supply-Chain Attacks Come to Light in Less Than a Week," Ars Technica (10/23/2018) - https://arstechnica.com/information-technology/2018/10/two-new-supply-chain-attacks-come-to-light-in-less-than-a-week/.

19 "The Risk IT Framework," ISACA (2009) - http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework_fmk_Eng_0610.pdf?regnum=.

analysis.[20] A common, effective, easy-to-use method is the five whys approach.[21] First, write down the problem you're analyzing. Then ask why; write down your answer. Then ask why your answer occurred. Keep analyzing until you've reached the root cause. Note that five is just a guideline. It might take three or it might take seven. The point is to find out the root cause. See figure 4 for an example.

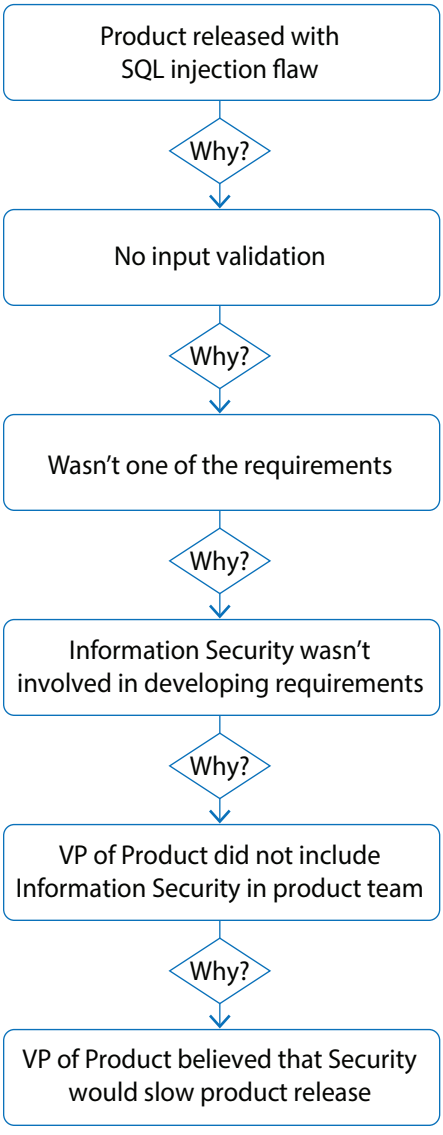

Figure 4 – An example root cause analysis

In this example, the root cause was product leadership's belief that Information Security would slow down the product release. This is likely a product of the organization's culture. It could also be based on experience, either within the current company or past companies or based on what he or she has heard from other companies. Note that in a dysfunctional blame culture, the developer or maybe the developer's manager would have been blamed, and the analysis would have stopped there.

The solution is education. The VP needs to understand the business argument for pushing or shifting left.[22] This means shifting security activities from the end of development phases to the beginning. The main business argument is cost: it's cheapest to fix bugs during the design phase of the software development life cycle (SDLC). As bugs are found later in the cycle, it becomes more expensive to fix them.

Potential solutions include automated static code analysis, security training for developers, and a security champions program. A cultural shift driven and sustained by upper management will help maintain these changes and improve security overall. Beware of implementing solutions in response to findings from an annual penetration test or to an incident and then letting the solution wither over time.

More generally, leadership needs to identify the security culture it wants and act to create it. Perhaps leadership wants the team to believe in the importance of being proactive, evolving processes, keeping up with the threat landscape, understanding organizational risk appetite, open communication about risk, and learning from incidents. Leadership needs to communicate these to staff, needs to model these attributes. That is, leadership can't be in the "blame game" yet expect others to learn from incidents. When teams demonstrate security in an exceptional way, management should publicly reward them. Performance of these cultural elements can be evaluated in formal reviews. Finally, metrics for each cultural attribute can be developed and tracked over time, and deficiencies can be addressed.

Key takeaways

To build a risk-based information security culture:

- Establish information security leadership in the organizational structure that makes sense; ideally, the CISO should report to the CEO.
- Develop a strategy for transforming your security program into a risk-based program. The strategy will vary by company, but ad hoc and compliance-based programs are insufficient to defend against today's threats.
- Use ISACA's RiskIT guidance for creating a risk-based culture. Top leadership needs to communicate its risk appetite, drive behavior consistent with policy, and create a culture that learns from mistakes.

Conclusion

Technology-centric approaches still dominate information security programs. Excellent technology is needed to defend against the types and frequency of attacks today. However, it's not enough. Organizations need to attend to all three elements of one of fundamental security: people, process, and technology. Many organizations are not investing enough resources into building a robust information security culture, one that is risk-based. A strong information security culture will help all staff better understand security and integrate it into their thinking and behavior. Such a culture should reduce security incidents and help staff build security into their processes and projects. In such a culture, team members are more likely to notice emerging potential risks and remediate them before they result in damage.

About the Author

Don McKeown is currently an Information Security Manager at Wolters Kluwer Health. He earned an MBA with Distinction from Bentley University and holds the CISSP, CRISC, and GIAC Security Leadership (GSLC) certifications. He's available at don@donmckeown.net.

20 "Root Cause Analysis," Washington State Department of Enterprise Services - https://des.wa.gov/services/risk-management/about-risk-management/enterprise-risk-management/root-cause-analysis.

21 "The Five Whys: Root Cause Analysis," Pelletier Consulting (2014) - http://www.doe.mass.edu/acls/cp/referenced/5Whys-p24.pdf.

22 Kelley Bryant, "The Art of Pushing Left in Application Security," ISSA Journal (January 2019) – https://www.bluetoad.com/publication/?i=556006.