Instilling a Culture of Security Starts With Information Governance

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2vFygbZ

Change is difficult. Fear of the unknown, weariness of new approaches and apathy are change barriers individuals face in their personal lives and at work. In a corporate setting, these obstacles are exacerbated by the sheer number of people impacted, geographic factors, and reliance on existing systems and processes for continuity. Often, culture can be the underlying culprit to making important changes within an organization. Existing culture, whether official or perceived, can be a real hurdle to effectuating and implementing change. It is further complicated when dealing with compliance, privacy and security issues, given their sensitive and legal nature.

Corporations in highly regulated industries or with global operations face countless challenges in maintaining compliance with regulations and securing their data and the sensitive data they house on behalf of customers. In the United States alone, sanctions imposed on the private sector by regulators have steadily increased, and numerous class action lawsuits have been filed against corporations following major breaches of customer data. A Cisco report from 2016 found there were 780 breaches with a total of nearly 178 million records stolen in 2015, and the average cost of each lost or stolen sensitive record increased six percent from 2015 to 2016.[1] Adequately preparing for regulatory inquiries and litigation and arming against data breaches are complex endeavors that must be approached holistically and strategically. All of this begins with proactive and strategic information governance (IG).[2]

In practice, IG remains ethereal and abstract, with very little consistency from person to person on how it is defined. Broadly, IG is the practice and framework of proactively managing the valuation, creation, storage, use, archival and deletion of data within an organization. Efforts may also include migrating to cloud systems, establishing data privacy programs, implementing legal hold and enabling stronger regulatory compliance. Proactive IG allows legal, compliance and IT teams to take incremental, measurable steps toward bolstering programs, policy and culture shifts that are rooted in security and compliance and are necessary for dealing with today's data challenges.

A company that is facing privacy and security challenges does not need to radically change the way it does business, but rather can leverage culture to implement and foster the necessary procedural and technological transformations needed to strengthen security. Certain steps can be taken to build a strong respect for and practice of security into the cultural fabric of any organization, across all departments and areas of the business. Company activities such as moving to the cloud, responding to data requests for litigation or regulatory inquiries, staff training and education, and employee use of personal mobile devices for work can all significantly impact security and must be considered as part of efforts to strengthen the overall security culture. Executive leadership, strategic change management, technology implementation, incentives, customized training, mobile policies, and involvement of legal and compliance in executing IG and data security programs can all help shape a culture of security that is sustainable long term.

T. Sean Kelly
Is a senior director within FTI Technology's information governance and compliance services practice. He advises clients on all aspects of e-discovery and information governance, with a particular focus on developing and implementing legal-hold processes and technology and the legal impacts of migrating to Microsoft Office 365. He leverages more than a decade of experience in both legal technology and litigation support to advise clients on evolving technologies and the shifting landscape associated with cross-border transactions for global enterprises. Kelly previously worked for Johnson & Johnson, where he was responsible for e-discovery issues across business sectors, advising internal stakeholders and outside counsel on best practices in collection, forensic technology, document review and controlling cost.

Establishing a Task Force

First and foremost, any effort geared toward making changes to the corporate culture or implementing new IG practices will require a cross-functional team of key stakeholders that may include records management, legal, compliance, security, IT and operations. The task force will be instrumental in ensuring that new programs—and cultural shifts—are meeting the needs of the entire organization and addressing challenges that may arise from any given department.

Executive Sponsorship

Once key stakeholders are on the same page, they must secure board and/or executive sponsorship for the effort. The key to gaining buy-in is communicating the program's benefits that will specifically address the executive's unique pain points. If the executive sponsor is the general counsel, building the risk case for that person is critical—this includes the risk of not disposing of data that have met their retention requirement and are not subject to legal hold. If sponsorship is solicited from the chief information officer or another IT leader, he/she may be more likely to embrace a project that addresses data minimization and defensible disposal. Business leaders and board members will be more focused on the costs, overall impact to the bottom line and mitigated risk. The proposal should also take into consideration the cost avoidance of possible data breaches and penalties for failing to comply with various regulations in any region where the company does business.

Structure and Fresh Thinking

With executive sponsorship secured, the team must analyze the current infrastructure, policies and processes. This includes evaluating systems, how they are used in day-to-day operations, and employee attitudes toward security and compliance in the current environment.

> **“Any effort geared toward making changes to the corporate culture or implementing new IG practices will require a cross-functional team of key stakeholders.”**

Often, change goals get lost in a sea of discussions about headcount and resourcing requirements. But the people part of the equation is essential to enabling long-term transformation. According to a 2014 information governance survey, only 8 percent of organizations report that records management metrics for electronically stored information are mature, and only an additional 29 percent report that those metrics are improving.[3] To improve these metrics, organizations must invest in existing staff, while also bringing in new people who embody and demonstrate the values that will be part of the new culture. The introduction of new thinking and ideas, managers with a unique perspective, and experts with innovative strategies will lead to companywide behavioral changes that can refresh and renew the culture.

Incentives

A key part of gaining companywide adoption for any new program is to help employees understand what is in it for them. This can help affect behavior and attract new capabilities. There are a handful of household-name companies that are known for maintaining strong incentive programs that are directly linked to company culture. What their approaches have in common is linking performance and monetary incentives to an evaluation of how employees are living and acting by the cultural guidelines.

> “When rolling out any new program, it is imperative to have a computer-based training module in place for all users.”

By understanding what incentivizes people and linking those incentives to employees’ active participation in embracing new processes, such as compliance and security protocols, IG stakeholders can significantly improve the enthusiasm and pace at which new culture standards are adopted. The IBM X-Force 2016 Cyber Security Intelligence Index reported that in 2015, 60 percent of all attacks were carried out by insiders, either those with malicious intent or those who served as inadvertent actors.[4] This is an important reminder of why security must be instilled from the top down, across the entire workforce.

Change Management

Understanding how to effectively manage and enable change—and approaching it as a journey toward stronger security and compliance—is essential. During an effort to change the culture for stronger security awareness, the task force must communicate the fundamental legal and regulatory drivers behind the proposed changes and ensure the company understands just how important these factors are to the organization’s overall success and business continuity.

One of the most widely accepted methods for implementing change management is the Kotter 8-step Change Model,[5] which was developed to help organizations become adept at progress. Some of the key tenets of this model, which will help with strengthening attitudes toward security, include creating urgency, clearly communicating the vision, identifying and eliminating obstacles, setting short-term realistic goals that foster a sense of achievement among those involved, and making changes permanent by solidifying adoption and addressing opposition head-on. These steps can again be tied to incentive programs to provide employees with attainable goals that align with the new security programs.

Training

When rolling out any new program, it is imperative to have a computer-based training module in place for all users. The information governance survey mentioned earlier reports that half of organizations indicate employees never receive records information management training.[6] Executive sponsors can be particularly helpful in ensuring that the training is mandatory for everyone in the organization—a key factor in maintaining long-term change. Outside advisors can be particularly useful at this stage, as they are able to help internal teams outline the critical security vulnerabilities and necessary components of the program, develop audience-specific training materials, identify what users will need to be trained on, and determine what the depth of that training should be.

Training should not be out of the box from software providers, nor should it necessarily be the same for everyone in the organization. Training collateral should be security- and privacy-focused and tailored to the organization’s specific needs. Materials must show users what the new policies look like within the context of their work environment and how they impact data breach prevention and regulatory compliance. It is also useful to build a dedicated page available to all internal users that offers reference guides and a frequently asked questions section dedicated to explaining new policies and tools that are being used and why.

Mobile Workforce

The entrance of the Internet of Things (IoT), mobile devices and text messages into the world of e-discovery has created a number of challenges that impact compliance and security. Data on a custodian’s mobile or Internet-connected device, including text messages or other data that have been collected from the device—whether company owned or personal—might be in scope in almost any investigation or litigation and can be more vulnerable to a data breach or leaks. These devices are evolving especially quickly, and architecture and software tools that are new today may be antiquated tomorrow. Corporations that are proactive about both their mobile workforce and any company-related usage of IoT products and maintain up-to-date and enforceable policies will find it much easier to navigate compliance and security issues. IoT specifically should be vetted by IG stakeholders within an organization to determine possible risk areas and how data from those devices may need to be mitigated.

Another related and growing area of consideration is enterprise migration to cloud services such as Google Apps for Work and Microsoft Office 365. According to Microsoft, Office 365 alone has more than 60 million commercial customers, and adoption is expanding at a rate of 50 percent quarter over quarter.[7] The movement of critical corporate data to the cloud raises security and data protection concerns, and analyst reports have shown the incidence of advanced email threats rising for corporations of all sizes. IBM reported that the average client organization monitored by its Security Services experienced 52,885,311 security events, 1,157 attacks and 178 incidents.[8]

Cloud migration brings a long list of IG priorities and considerations, ranging from e-discovery needs, retention and legal hold requirements, migration methodology, and technical quality control and testing. These issues are complex and should be addressed in advance of a migration to ensure proper handling across IT, legal, compliance and security, and to build in training and change management that map back to the broader efforts of weaving security into the company's culture. When looking at policies for mobile device data, counsel should address data privacy concerns and software limitations for managing security. Key considerations include:

> **"Maintaining change and enforcing adoption of new processes is critical to shaping a culture of security that grows and strengthens over time."**

- **Device ownership**—Making a distinction about who owns the device and what access the organization has to the data on that device is important and must be outlined by an acceptable-use policy that applies to all devices and gives consent for the company to control the device through mobile device management, including remote access, data collection and wiping the device.
- **Data privacy**—Multinational corporations must be mindful of the wide variety of data protection laws around the globe and prepared to deal with conflicts between privacy laws and corporate policies in regions where the data reside; development of individual policies that are tailored to the data protection laws of each region can help lay the groundwork for securing data in compliance with each jurisdiction.
- **Software**—Every company should have mobile device management software in place, which eases some of the challenges with securing, managing

Enjoying this article?

- **Learn more about, discuss and collaborate on information security policies and procedures in the Knowledge Center.** *www.isaca.org/information-security-policies-and-procedures*

and collecting data from mobile devices; the software should offer strong scalability to grow as the company grows and provide features that allow the corporation to control the device on the back end without visibility to users.

Enforcement

Maintaining change and enforcing adoption of new processes is critical to shaping a culture of security that grows and strengthens over time. There are a handful of approaches and technologies that enable compliance monitoring, and they work by flagging violations of new protocols and enabling stakeholders to take remedial action. In conjunction with monitoring, tying compliance to employee performance evaluations is very effective to driving adoption. When employees understand that a lack of participation with training programs or violation of new policies will adversely impact their performance ratings or compensation, they are much more likely to dig in and commit to the changes. Employee metrics for compliance with new policies can be directly tied to the organization's incremental goals for implementing those policies and measuring adoption.

Education around how detrimental security breaches can be and the cost they impose on the organization can also help employees understand the negative impact. In many cases, it is not that employees are ambivalent about security; it is that they simply do not understand how their actions impact data security, nor how consequential a breach can be. Once they have been educated about the overall importance of security to the long-term health of the company, most employees are much more supportive of security efforts and are vigilant in reporting policy violations.

Conclusion

Failure to handle data properly and instill a deep respect for privacy and security can result in damaging data breaches, and it has for hundreds of companies. Beyond the legal and compliance risk that comes with a data breach, it also breaks trust and causes doubt to become part of the company's reputation. Thus, it is critical that the legal, compliance and security requirements are viewed as opportunities to instill a high standard for ethics and privacy into the company's culture.

When each and every employee embodies trust, ethics, security and privacy, these values will translate to the services or products the company provides. By embracing this mindset, a corporation's leadership can set the correct tone from the top down, building advocacy for actionable programs that ensure safe and responsible handling of sensitive data, in addition to strong compliance and efficiency.

Endnotes

1 Cisco, *The Zettabyte Era: Trends and Analysis*, 2016, *www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.pdf*

2 FTI Consulting, "Information Governance & Compliance Services," *www.ftitechnology.com/solutions/information-governance-and-compliance-consulting-services*

3 Cohasset Associates, ARMA International, AIIM, *2013 | 2014 Information Governance Benchmarking Survey,* 2014, *www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/White-Papers-Briefs/C/Compliance-Benchmark-Report.aspx?TempAuth=True*

4 IBM, *X-Force 2016 Cyber Security Intelligence Index*, 2016, *https://www.ibm.com/security/data-breach/threat-intelligence-index.html*

5 Kotter International, 8-step Process, *https://www.kotterinternational.com/8-steps-process-for-leading-change/*

6 *Op cit,* Cohasset Associates

7 Microsoft, "Microsoft Cloud Strength Highlights Third Quarter Results," 27 April 2017, *https://news.microsoft.com/2017/04/27/microsoft-cloud-strength-highlights-third-quarter-results-2/#11Ct2akfPsVWgmyz.97*

8 *Op cit,* IBM