BankDirector.com CHARTING A COURSE FOR AMERICA'S BANKING LEADERS

Effective Cybersecurity Demands Involvement From Everyone at Your Bank

By: *Troy La Huis, Dave McKnight* | JULY 10TH, 2018

Cybersecurity is one of the most discussed risks facing financial services companies today, but many organizations are taking too narrow an approach to combating cybercrime. These organizations make the mistake of placing responsibility for defending against the risks solely on their IT professionals.

As criminals continue to develop increasingly targeted attacks, institutions must tackle cybersecurity from an enterprise-wide perspective that goes further than mere regulatory compliance. Cybersecurity can no longer be the function of a single department–executives must see that it is embedded throughout the enterprise, from the branch to the boardroom.

Common Cybersecurity Gaps

Even institutions that have invested funding, allocated resources, built perimeters, and complied with regulations can fall prey to a single point of cybersecurity failure. Some of the recent major attacks have resulted, at least in part, from one of the following fail points:

- Poor governance
- **Weak passwords**
- Inaccurate monitoring or unattended security information and event monitoring functions
- Inadequate system patching procedures
- **Lack of cyberintelligence** (external information gathered on known attacks)
- Insufficient training
- Lack of incident response planning

Notably, **vulnerabilities such as weak passwords and insufficient training involve more than just IT staff**. Organizations that involve all departments empower their employees and think daily about how their actions protect or expose the organization, and translates into multiple points of control. Strong governance is, of course, essential to achieving such an embedded mindset.

The Need for a Tailored Approach

Many financial services organizations have responded to cyberthreats by investing heavily in costly, one-size-fits-all technology systems. They rely on traditional controls for protection, like firewalls, encryption, anti-virus software, and multifactor authentication. These components are helpful and most often are necessary; however, many institutions require more tailored controls and processes. Instead, organizations should adopt enterprise-wide cybersecurity programs commensurate to their particular risks and sensitive assets.

For example, it's common for a financial service organization to provide employee training on cyber risks. But standardized, "off-the-shelf" training does not consider the varying degrees of risk across the staff population. For training to be meaningful, it must be customized to different employees' roles and access to data.

To develop such training, as well as other appropriate controls, **an organization will need to identify the assets it wishes to protect and the associated access points**. Each department or business unit that maintains sensitive information must catalog the information and classify the sensitivity of each asset, taking into account the organization's risk appetite (the acceptable level of risk exposure). The departments then should identify all methods of access to each asset, as well as the parties with such access, and quantify the resulting risk.

Only when armed with this information can a financial services organization tailor appropriate controls and properly allocate resources against the related cyberthreats. For example, most organizations do not need to treat data across the enterprise equally. Rather, they can define unique security controls for the most sensitive data. Similarly, it might be wise to **institute the most comprehensive training in the departments with access to sensitive data, are customer-facing, or those who provide information to third parties on behalf of the organization**.

Enterprise incident response is another area that calls for a more customized. An organization should identify employees best positioned to notice suspicious activity and ensure they know how to respond. IT employees who are monitoring account and system activity should be included in this process, but key stakeholders and employees who are client and third-party facing also should be involved. The organization also must have an appropriate response plan ready to execute when those on the front lines raise the red flag.

Critical Steps

To adopt an enterprise-wide cybersecurity program, financial services organizations should:

- Identify and prioritize sensitive assets.
- **Design and implement tailored and global controls** aligned with sensitive assets and their associated risks (including dual controls for especially sensitive areas).
- Ensure executives and the board are aware of and aligned to the tailored program, which includes making cybersecurity part of the overall strategy of the institution.
- **Educate employees** specific to their roles and the associated.
- Manage cybersecurity at the enterprise level and on employee devices.
- Continuously monitor significant areas and environmental changes.
- Keep software and systems up to date.

Multiplying the Benefits

Financial services organizations that take a broad view of cybersecurity establish more effective and cost-efficient controls. Moreover, organizations with all of their employees on the same page are more likely to enjoy improved performance.

Troy La Huis is a principal with Crowe LLP and can be reached at (616) 233-5571 or troy.lahuis@crowe.com.

Dave McKnight is a senior manager at Crowe LLP where he leads the firm's cybersecurity incident management group. He works with mid-to-large tier financial service organizations to refine their cybersecurity capabilities.