Forrester's 2011 security strategy recommendations

How to take a more systematic approach to governance and data protection even as the computing landscape continues to change

http://www.csoonline.com/article/657814/forrester-s-2011-security-strategy-recommendations

By Khalid Kark

January 25, 2011 — CSO —

Every New Year brings an opportunity to review existing security plans and adjust strategies for the next year. And, as I participate in these conversations for 2011, a lot of similar themes have popped up. Most CISOs are struggling with the same issues, ranging from dealing with the changing threat landscape to properly supporting the rising adoption of social technologies, employee-owned mobile devices, and cloud services. In fact, Forrester's research shows that a majority of challenges for security professionals all relate to business orientation and alignment. For example, many senior business and IT leaders are asking CISOs to better support and align with the business and IT objectives, requesting regular interactions and updates from security teams.

Given security leaders' pain points and focus areas for 2011, Forrester has identified recommendations for security strategies that address the broad security trends in the current market. Our recommendations fall into three major themes: 1) better governance structures; 2) more mature security processes; and 3) improved analytics and reporting capabilities.

Develop Governance Strategies To Support An Empowered Organization

Social, mobile, and cloud technologies are part of a groundswell movement that has taken hold of organizations, propelling waves of innovation and business transformations. Security can no longer block or impede this momentum; rather it's time for security leaders to mitigate risk to a level that is acceptable to the business. This means security leaders need to:

- **Prepare for social technology adoption.** As one CISO put it, social media adoption is like a freight train coming; if we don't prepare ourselves for it, we'll get hit pretty hard. Forrester surveys show a dramatic increase in the number of people accessing social media Web sites every day—the numbers have jumped from about 11% in 2008 to 30% in 2010. Social media technology increases the risk of malware infections and data leaks (both intentional and unintentional). Social media policies will have a wide variation, but it's important to have a governance strategy and specific policies in addition to the technical controls, process checks, and people awareness to mitigate this risk.
- **Help the business devise a strategy to leverage cloud services.** The cloud is here to stay, so while security leaders should raise concerns about data security and regulatory risks, they should also be recommending ways to mitigate these risks of data disclosure or a data breach.
- **Actively support mobility in the post-PC era.** As devices such as tablets, eReaders, and smartphones eclipse PC devices like desktops, laptops, and netbooks, security and risk professionals must aim to bring a measure of control to an increasingly chaotic environment, while maintaining employee flexibility and innovation.

Mature Existing Processes To Enhance Data Protection Capabilities

A major theme emerging for CISOs in 2011 is the desire to understand and measure the maturity of organizational processes. With the changing threat landscape, many security professionals have found existing processes to be inadequate or inefficient. Many CISOs I talked to are developing more consistency and rigor to validate regulatory compliance requirements as well as adherence to standards such as NIST, ITIL and ISO 27001. Although better maturity is required across all security processes—here are the especially important moves to consider:

- **From reactive tools to proactive focus on integrating tools and processes.** During a recent conversation, a security system integrator claimed that 95% of their clients chose to deploy IPS rather than IDS. Although this statement was not shocking, it does highlight a general trend: the realization by security professionals that an ounce of prevention is worth a pound of cure. Organizations are moving away from blindly deploying reactive technologies to deploying preventive processes and technologies or by enabling the preventive features on their existing technologies.

- **From identity management to information and access management.** As companies focus on securing their data, security professionals need to recognize that's it's not just about managing identities, but that access control and information management are key components of data security. The proper management and control of user accounts, access permissions, and privileges is one of the most effective avenues to ensuring data doesn't walk out the door.
- **From ineffective incident planning to robust breach response.** Having a comprehensive and well-tested breach response plan could be the difference between a contained incident and a front-page fiasco. And with the increased sophistication and targeted nature of threats, coupled with their increasing frequency, sooner or later there will be a security incident to handle. Security professionals should be prepared.

Build A Competency In Analytics For Improved Visibility, Metrics, And Decision-Making

Many CISOs admit that finding relevant information from the constant data stream is like finding a needle in a haystack. CISOs need to ensure that metrics and reporting efforts focus on three levels of decision-making: operational, risk, and business-centric. [Editor's note: See Security metrics: Critical issues.] And each level requires a different type of data to fulfill their job. Once security professionals start measuring in their own environment, it may be appropriate to look at industry benchmarks for comparison:

- **Educate and equip risk owners with relevant information for decision-making.** Avoid being one of the many security organizations that don't use any kind of formal risk management discipline to objectively identify, analyze, and assess risk. This will help reduce any underestimates, or exaggerations of risk. Remember, it's the CISO's job to enumerate the risks of the business, but it's up to the business to make the final decision on the acceptable level of risk.
- **Demonstrate the value of security with business and financial metrics.** It's important to note that C-level execs and board members most likely don't care about the security team's operational metrics. They're far more concerned with the organization's overall risk posture. In fact, many are savvy enough to understand that there's no real ROI for some security investments; so they're looking instead for maturity models and risk frameworks to understand how the investments are changing their risk posture.
- **Enhance operational measures through validation and correlation.** Implementing a security technology is the easy part. Ensuring that it's continuously and consistently working is much more difficult. One company that was sending most of its alerts and events into its SIEM tool was hacked because one of the rules on the SIEM was misconfigured. The tool didn't even peep as the hackers breached the environment. Many CISOs complain that the sheer volume of information they need to sift though is overwhelming, and they're turning to correlation capabilities of SIEM tools. However, unless you're testing and validating these controls, even the best security technology in the world is useless.

Information Security Strategies Found Lacking: PwC

http://www.cioinsight.com/c/a/Security/Information-Security-Strategies-Found-Lacking-PwC-322139/

- 43% of respondents think their company has an effective information security strategy in place and are proactively executing their plans.
- High confidence – 72% of respondents report confidence in the effectiveness of their organization's information security activities.
- Few leaders - Only 13% of respondents prove to be true information security leaders
- Meaning that they have: An overall information security strategy in place, a CIO or executive equivalent who reports to top management, measured and reviewed security policy effectiveness, and an understanding of the security breaches facing the organization in the past year.
- Getting personal – 43% of respondents say their company has a security strategy for employee use of personal devices.
- Mobile strategies – 37% of respondents say they their company has a security strategy for mobile devices.

- Social security – 32% of respondents say their company has a security strategy in place for social media.
- Cloud's impact – More than half (54%) of respondents say that cloud technology has improved security, while 23% say it has increased vulnerability.
- Big driver – Many respondents (including 64% in industrial manufacturing, 60% in technology and 49% in entertainment and media), say the existence of an Advanced Persistent Threat (APT) is driving their organization's security spending.
- Only 16% of respondents say their organization is prepared for an APT and has security policies that are able to confront such a threat.
- Unusual suspects? – 17% of respondents identify customers as the source of security breaches, and 15% identify partners or suppliers as the source.

Other Interesting links

Provided for reference and interest. Not intended for you to review prior to the governance meeting.

- TED Talk: "Bruce Schneier: The security mirage" [21 min]
  http://www.ted.com/talks/bruce_schneier.html
- TED Talk: "Mikko Hypponen: Fighting viruses, defending the net" [17 min]
  http://www.ted.com/talks/mikko_hypponen_fighting_viruses_defending_the_net.html
- Internet 2 Wiki - Information Security Governance
  https://wiki.internet2.edu/confluence/display/itsg2/Information+Security+Governance
- Developing an Information Security Strategy & Program
  http://infosecbyac.blogspot.com/2011/10/developing-information-security.html