

Focus Experts' Briefing: How CEOs Can Prepare for and Respond to Cyberattacks

July 26, 2011

Focus Experts included:

John Anderson

Andrew Baker

Kevin Beaver

Brian McCallion

Barry Schrage

Richard Stienon

Focus Experts' Briefing: How CEOs Can Prepare for and Respond to Cyberattacks

How should CEOs prepare for and respond to cyber attacks?

topics: [Expert Briefing](#) [Expert Content](#) [IT Security](#) [Information Technology](#) [Cyberattacks](#)

Executive Summary

Cyberattacks are a certainty in 2011. As Focus Expert Andrew Baker cautions, "Cyberattacks are a virtual certainty at this time — whether targeted or scripted. ... There are so many script kiddy attacks that are floating across the Internet at any given time that no organization should expect to avoid getting hit." Focus Expert Kevin Beaver adds: "We're going to have to get past the mindset that information security is an IT issue. It's not — it's a business issue." And, as with all business issues, support for cybersecurity must come from the top-down. In this guide, Andrew, Kevin and their fellow Focus Experts John Anderson, Brian McCallion, Barry Schrage and Richard Stienon share their advice on how CEOs can prepare for and respond to cyberattacks.

After reading this guide, check out the entire discussion and join the conversation: <http://focus.com/c/HVT/>.

Expert Advice

1. Evangelize cybersecurity to senior executives.
2. Appoint a 'Cyber Commander' to oversee defenses against targeted attacks.
3. Use US Defense Information Systems Agency checklists as a model for your security review.
4. Embed cyberattack defenses in disaster recovery and business continuation processes.
5. Enlist external experts to review your security system and the code.

Focus Experts' Briefing: How CEOs Can Prepare for and Respond to Cyberattacks

How should CEOs prepare for and respond to cyber attacks?

1. Evangelize cybersecurity to senior executives.

"CEOs should make it clear that investing in cybersecurity is expected of their senior executives and cannot be ignored. This investment must include a directive to the information technology organization that they must invest money and energy into securing their systems to the highest level possible and, if applicable, meet whatever compliance standards apply to their industry. Did you know that the vast majority of those sites — 79 percent, according to the Verizon Data Breach Report — that were breached and were subject to the PCI standard had not met that standard at the time of the breach?" (Schrager)

"They should take full responsibility and institute a policy that senior executives for each line of business sign-off on a standard suite of automated security tests and 'white hat' penetration tests before allowing an application or an update to an application to go live. Otherwise, it's see no evil, hear no evil, speak no evil. Unless the CEO makes it absolutely clear that security is a mission-critical quality of an application and that security issues directly affect people's careers at the company, the CEO should take full responsibility for any security issues. Otherwise, ignoring security issues is a way of saving short term expenditures, against which large a payout may need to be made. In this sense, it seems like it's a fiduciary responsibility of management to budget each quarter for security compliance. Otherwise, the shareholders end up with a 'steamroller' type event, much like an earthquake or another natural disaster against which the company has paid no premium and must suddenly charge to the business as if such events were unanticipated and/or under control." (McCallion)

"Executives must get on board and stay on board with security. Sure, it's up to everyone in IT and across the business to keep them abreast of what's taking place, but we've been doing that for years...decades. I know it's easy for me to make blanket statements that, in reality, don't apply to all executives. But what exactly does it take? How many breaches? How many lawsuits? How much eating crow? Only executives can provide the political and financial backing necessary to make this stuff work." (Beaver)

2. Appoint a 'Cyber Commander' to oversee defenses against targeted attacks.

"CEOs should institute a new role within IT: the Cyber Commander. The title could be changed, but the point is that countering targeted attacks is far different than today's operational security requirements of vulnerability scanning, patch management, AV, firewalls and IPS. The cyberdefense team must use special purpose tools to root out incursions, prepare for DDoS defense, research the malevolent actors that target the organization, and be ready to respond 24/7 to attacks." (Stiennon)

"As others have suggested, a comprehensive plan needs to be developed, led by someone on the senior team, who will drive the full spectrum protection, auditing and assessment activities of the organization's infrastructure and applications. Without an inventory, asset classification and risk assessment, there can be

no effective security program. And, most importantly, security mitigation activities must be embedded into the organizational DNA, and must have as much priority as revenue generation activities at all levels.” (Baker)

3. Use US Defense Information Systems Agency checklists as a model for your security review.

“If applicable to their systems, the US Defense Information Systems Agency (DISA) has its Security Technical Implementation Guides (STIGs) for the various systems they use within the US Department of Defense (<http://iase.disa.mil/stigs/>). While the checklists in these guides may not be totally applicable to every organization, they are an excellent start for an internal security staff to review their organization’s systems against.” (Schrager)

4. Embed cyberattack defenses in disaster recovery and business continuation processes.

“Cyberattack defenses need to be an integral part of not only IT’s cybersecurity process, but also embedded in the disaster recovery, risk management and business continuation processes. Today, there are so many more elements to security than even 10 years ago. Physical security is as important as electronic security and the combination must be considered in the IT strategic plan. Types of back-up systems, both on-site/off-site storage of mission-critical data and ‘time to recover’ are all important pieces. I see the CEO’s job here as ensuring that all these elements are in place, and that they are appropriately sized and costed for the size, customers and mission of the business.” (Anderson)

“CEOs need to take this class of threats as seriously as they would the defection of customers by way of departing sales agents/managers. Too many organizations look at cybersecurity in the same way that they look at contingency planning for earthquake or civil unrest in a Western country — i.e., as something that is not likely to occur, but for which it would be a good idea to have some preparation. However, cyberattacks are a virtual certainty at this time, whether targeted or scripted. Even if we exclude hacktivists and other politically motivated attackers, and even if a particular organization does not have direct financial resources tied to its website, there are so many script kiddie attacks that are floating across the Internet at any given time that no organization should expect to avoid getting hit.” (Baker)

5. Enlist external experts to review your security system and the code.

“Bring in external experts for both security assessments to assure that the system and its security are configured properly and also to review the system integrity of the code executing on the system. Unfortunately, recent surveys have shown that the largest security threats and actual breaches are coming from the inside — employees and contractors — and these are the people who are in the optimum position to leverage system integrity vulnerabilities for their own personal gain and leave no trace of their activities.” (Schrager)

Read the entire discussion, and join the conversation: <http://focus.com/c/HVT/>

Contributors



John Anderson

Principal, The Glowan Consulting Group
Focus Expert



Andrew Baker

Director, Service Operations, SWN Communications Inc.
Focus Expert



Kevin Beaver

Independent Information Security Consultant, Author, Expert Witness, Professional Speaker, Principle Logic, LLC
Focus Expert



Brian McCallion

President, Bronze Drum Consulting, Inc.
Focus Expert



Barry Schrager

z/OS Information Security Leader & Architect
Focus Expert



Richard Stiennon

Chief Research Analyst, IT-Harvest
Focus Adviser

About this Report

Focus Experts' Briefings are sourced from Focus Experts who have exhibited expertise in the particular topic. Focus Experts' Briefings are designed to be practical, easy to consume and actionable.

About Focus

Focus.com makes the world's business expertise available to everyone. At the heart of Focus is a network of thousands of leading business and technology experts who are thought leaders, veteran practitioners and upstart innovators in hundreds of different topics and markets. You can connect with the Focus experts in three primary ways: Q&A, Research and Events. Personalize your Focus.com experience by following specific topics and experts and receive the Q&A, research and events of interest to you. Focus is easy to use and freely available to anyone who wants help making better business decisions.