PLURALSIGHT

Pluralsight Offers CEOs Five Security Tips to Prevent Cyber Attacks

Global e-Learning Leader Suggests Ways Executives Can Prepare for and Prevent Digital Breaches for Companies Worldwide

SALT LAKE CITY (June 17, 2014) – Pluralsight, a global leader in online training for technology professionals, today released five recommendations for top executives to prevent security breaches. Following recent high-profile hacks at major companies such as Target and eBay, as well as the widespread panic inflicted by the Heartbleed Bug, the tips aim to help organizations with a digital presence—including websites, point-of-sale terminals and software companies—protect their businesses and keep information secure.

"The cost of a security breach can not only negatively affect a company's reputation but also consumer confidence and even revenue," said Troy Hunt, security expert at Pluralsight. "In most cases, the vulnerabilities that lead to these attacks are already known within the technology industry, but it's a lack of process and awareness that results in them being exploited. It is paramount that companies understand what pre-emptive measures to take before an incident occurs, as hacks can cost companies billions of dollars and even cause companies to fold."

Below are five tips from Hunt to help top executives prevent cyber attacks and mitigate harm in the event a breach does occur.

1. **Do not rely on security audits alone.** While standards such as PCI DSS (the Payment Card Industry Data Security Standards) encourage security compliance to rules and regulations, these standards are infrequently assessed, rarely exhaustive and can easily be compromised by simple oversights in processes. A successful audit often leaves a company feeling "secure," but it is not a foolproof measure for company security.

2. **Let the IT department's security culture play an important role.** Security management is an ongoing process, and an organization's culture and approach to security can show its propensity for risk in being attacked. The following questions can help ensure IT maintains a culture of security:

- Do software developers and IT professionals working on building systems undergo any formal security training?
- Are there dedicated security professionals involved in assessing the IT landscape?
- Are there regular penetration tests? Is there someone accountable— such as a Chief Information Security Officer—who is shepherding these processes?

3. **Make sure security is not simply implied.** Following a security breach, many organizations respond that they believed the system was "secure." However, as the implementation of these systems is entrusted to partners or staff, the definition of "security" is often vaguely defined and can be misinterpreted. Expectations should be explicit and clearly spelled out as part of the system requirements to prevent the exploitation of security risks. Wherever possible, security standards should be defined as a requirement of the system, as should the processes that assess these standards and ensure compliance.

4. **Understand security is a balance, not an absolute state.** A common fallacy with security is that a system is either "secure" or "insecure," but any system will eventually fall to a determined attacker. Organizations must focus on defining the balance between what is being protected, who it is being protected from, and the overall impact a breach will have, and strive not for an ultimate state of "secure," but rather "secure enough" for

their unique circumstances. In addition, vulnerabilities and risks will evolve over time, and security controls need to adapt accordingly.

5. **Communicate early and clearly in the event of an incident.** Even when all reasonable measures are taken, security incidents do still occur. When a system is compromised, customers are often left wondering about the impact, leading to speculation that adversely affects a company's reputation. Communicating with customers early is essential, and failing to do so promptly, clearly and concisely after a breach can be detrimental to a brand. In order to avoid confusion, organizations can develop an incident response plan that addresses who takes responsibility for a breach, how it affects customers and how to minimize the potential damage to the organization.

"Attacks against IT systems are inevitable, but a company's preparedness can determine how successful breaches are and how much impact they ultimately have on the business," Hunt added. "CEOs can start with these five points to ensure the IT department understands the value of security — not just the cost — to keep its data, businesses and reputation safe."

For more information on web security training visit
http://pluralsight.com/training/Courses/Find?highlight=true&searchTerm=online+security

About Pluralsight
Founded in 2004, Pluralsight is the global leader in online learning for professional software developers, IT specialists and creative technologists. As the world's largest curated professional development platform, the company offers instant access to more than 4,000 courses authored by top experts. With customers in more than 150 countries, Pluralsight serves as a career catalyst, delivering hands-on, practical training for the most in-demand and understaffed jobs of today. For more information, visit Pluralsight.com. or Digitaltutors.com.

###

Contacts
Pluralsight PR
Megan Herrick, VP of Communications
801-784-9135
megan-herrick@pluralsight.com

Katy Kenealy
801-828-6056
katy@methodcommunications.com