Top Security Pitfalls to Avoid in 2014

2013 ended with a bull’s-eye on an estimated 100 million Target customers, leaving many shoppers recovering from the holiday season much differently than expected. In fact, 2013 saw several successful high-profile hacks, including Adobe, JP Morgan, Yahoo, and LinkedIn. You can bet that 2014 won’t be any different! What can you do to protect your organization in 2014? Here are our thoughts.

Technology Trends
Arguably, the current theme of technology is “decentralization,” evidenced by the proliferation of mobile devices, social media, and the popular endorsements of both bring your own device (BYOD) and the “cloud.” All of these provide for the propagation of data outside the traditional borders of your control.

With these technologies, answers to questions like who owns the data, who’s responsible for protecting it, and how should it be protected are obfuscated by slick marketing practices; favorably written vendor contracts, service-level agreements (SLAs), and privacy policies; and fuzzy regulatory guidance. Suffice to say, decentralization will leave less mature and naïve organizations more vulnerable in 2014.

Suggestions for 2014:
Think before you implement. Implement technology based on the strategic direction of the organization, not a whim or desire for the latest new product. Also, incorporate security needs and implications in your implementation. If already implemented, realize your data may not be as secure as you think; revisit your contracts, SLAs, and user policies to understand your responsibilities. Invest in security — make it an independent line item within the annual budget. Don’t let departmental tunnel vision or hubris limit how you protect your organization and customer data.

Current Technologies
Similar to the large number of zero-day vulnerabilities in Java 6 found after Oracle ended support for the software in 2013, expect to see a sharp rise in attacks against Windows XP and Office 2003 users after Microsoft ends support in mid-2014. Many of our clients have critical legacy applications that require these unsupported platforms to operate, including ATMs, point-of-sale systems, healthcare devices, and other critical systems. In 2014 these systems will become even greater liabilities for organizations.

In addition, the Adobe source code leak in late 2013 will likely lead to a rise in email attachment and watering hole attacks against Adobe users and web applications. Less commonly known, but still quite dangerous, a watering hole attack is where a compromised website launches malicious code against anyone who simply visits the site, infecting the unsuspecting user’s device with malware.

Suggestions for 2014:
If not yet started, begin the transition from older and vulnerable technologies. If legacy systems or vendors become a hindrance, undergo a technology assessment to identify alternatives. Think beyond Microsoft — watch for security updates and patches from software vendors. Java, Adobe, ActiveX, and others are constantly issuing updates to help keep users more secure. Take an independent look at security. Consider penetration testing and security scanning to get an outside perspective of your current state.

User Behaviors:
Password reuse (the use of a single password to protect multiple applications like Facebook, LinkedIn, Gmail, Dropbox, PayPal, etc.) amplified the effects from the LinkedIn, SnapChat, LivingSocial, and other hacks in 2013. Hackers enjoyed a particularly frightening reality. These popular sites, once compromised, became treasure troves of usernames, email addresses, and passwords allowing them, through various methods, access to additional email accounts, social sites, and web applications like iTunes, Amazon, and PayPal. Phishing is yet another popular way in which hackers were exploiting user behaviors to gain access to organizational networks and personal user accounts in 2013. In general, people are idealists — impulsive and credulous, willing to help other people without first asking, “Why?” This is why users are, and will continue to be, the weakest link in security. In 2014 hackers will link the phish fodder harvested from social sites, subverted by hackers after high profile attacks, to weaknesses in current systems built on unsupported platforms and technologies in order to significantly increase the success rates of their attack campaigns.

Suggestions for 2014:
Educate, Educate, Educate!

In Conclusion:
By combining predictable user behaviors with weaknesses in currently deployed technologies and the proliferation of data in decentralized control environments, we anticipate 2014 will be rather eye-opening and costly for both companies and individual users. Organizations, employees, and individual users will learn how to protect themselves or unknowingly fall prey to hackers. Know where your data is, institute a 1-800-data-breach line to report breaches, and monitor access. It’s insufficient to rely on firewalls and antivirus software.