The 10s

Serious Insights

By Daniel W. Rasmus

Knowledge Management Ideas CIOs Should be Applying to Seal Cyber Leaks

1 **Education** If IT and non-IT staff don't understand the risks and the approaches used by hackers, then no amount of automation is going to keep data safe. Establish a program that puts everyone face-to-face with the threat and create assessments that demonstrate they get it.

2 **Do the simple stuff** Ensure that all devices used in the work environment, from PCs to phones and tablets, utilize adequate virus and malware protections. Monitor Microsoft's Active Directory and other directory services like LDAP. Restrict what can be run on servers, and ensure networks that shouldn't communicate can't communicate. Many breaches use common tools, social engineering and basic commands to extract data. Knowledge of what your systems should be doing, and what they shouldn't be doing, is key.

3 **Monitor behavior** Pay attention to new account creation, installed apps, running jobs, unusual commands and other activities that might be an indicator of a breach in progress. Good security monitoring trumps productivity in areas where automation isn't effective. Organizations must actively monitor their environment, if they don't, then their policies and promises don't reflect actual commitment. In the Target attack, it is reported that hackers used Microsoft PSExec and Remote Desktop, both of which can be monitored if people are watching.

4 **Guard against known vulnerabilities** If there is a known vulnerability in an app or browser, then actively monitor for evidence of exploit or remove the offending software.

5 **Force password changes** In an organization that maintains deep information about customers, a password change may be the difference between a breach and a failed attempt at "Pass-the-Hash." People hate changing their passwords, but if they know why, you can reduce the angst.

6 **Regularly review admin accounts** Require admin accounting on servers. In other words, know who has privileges, document them, and if new accounts pop up that don't match the people with the privileges, delete them quickly. Also avoid fake names and shared accounts.

7 **Design an IT security experience** IT experience design can take advantage of ideas from *Management by Design* like understanding what security is balancing for (the tension between security and productivity, for instance) and how to serve up variety to would-be hackers while providing guidance on what to pay attention to for employees and partners (emphasis). It is also important to ensure that policies and practices are followed and that communications, horizontal (perceptibility) and vertical (rhythm and motion) are open and effectively used. A well-designed environment won't stop an attack from starting, but it may well stop it from getting very far.

8 **Impose policies on partners** Organizational policies on passwords and other security related protocols should be contractually bound to vendors, inclusive of those who provide hardware, software and staffing. Breaches can start just as easily from a partner account as from an internal one.

9 **Join the Agency** Knowledge is the best way to thwart attacks on IT infrastructure. Join organizations like the IT Sharing and Analysis Center (IT-ISAC) and new Retail Cyber Intelligence Sharing Center (R-CISC), and read alerts from security software suppliers. Don't let the sense of sleuthiness deter IT professionals from getting involved in these organizations. The world of hacking is a dark one—those who want to avoid infiltration need to understand how it works and the tools of the trade.

10 **Good security is good knowledge management** Good knowledge management requires active monitoring and paying attention to the knowledge required to continuously deliver high quality goods and services. Ultimately, security practices should reflect good knowledge management practices like understanding how things function, making sure that people working with systems and technology regularly share their knowledge, insights and observations, that people actively monitor systems in order to discover emergent behaviors, and that they react to change through feedback loops before new approaches or apps become new opportunities for hackers.