Quest TECHNOLOGY MANAGEMENT

STRATEGIC ADVISOR

VOLUME IX, NUMBER 1

Why Continuous IT Security Monitoring Can Save Your Business

If you've found yourself giving the security of your business a second thought, you're not alone.

And for good reason: 2013 saw some of the most dramatic cyberattacks in Internet history — from the Snowden revelations and the hacks of Facebook, LinkedIn and Twitter to the breaches that exposed sensitive data of almost 40 million Adobe customers and 100-plus million Target customers.

A new Internet landscape

"Recent cyberattacks signal a sea change in the role of the Internet," observes Quest President and CEO Tim Burke. "We do business online anytime from anywhere, we shop online, we play online, we store our data in clouds — complex activities featuring a vast array of connections among uncountable devices and data that organizations' technology infrastructures must support. This has created what security specialists call 'a greater attack surface'."

Certainly, mobile devices — especially at work — have contributed to today's expanded attack surface. Analyst firm Gartner estimates that in 2014 the number of Android and Apple mobile device users alone will top 2.5 billion as PC, tablet and mobile phone shipments increase 7.6% over last year.

No one doubts that smartphones and tablets used to access cloud-resident data and engage social media have helped inspire the increasing sophistication of threats and attack models (see **Did-You-Know** on page 3).

So — how much should you worry?

"If your data has any 'street value,' someone somewhere will figure it out," Tim notes. "And that puts even smaller organizations' data at risk."

Tim compares this to a burglar contemplating which dwelling to break into. "Big houses have the most goodies — but they also have the sort of security that takes risk and effort to bypass. So if the risk and effort are low enough because security is weak, even the diminished reward of attacking a small place can pay off."

THE BOTTOM LINE

The IT security landscape is changing fast and no company is safe, regardless of its size. How well-defended is *your* business?

IN THIS ISSUE

Do you need to rethink your IT security?

FROM TIM BURKE...

When It Comes to Security, Know Thyself

"If you don't understand the risks, you don't understand the costs," security guru Bruce Schneier advised during a TED talk.

He was discussing security in the abstract — but it got me thinking about IT security in particular and the difficulty many executives face trying to determine if their organizations are safe from cyberattack.

The problem is that these conversations nearly always turn technical. Soon, a flurry of technology acronyms — confounding but apparently reassuring — begin flying around the room.

And, reports Schneier, it works. People, he says, will "respond to the feeling of security and not the reality."

So what can a CEO do to understand the reality of security risk and grasp what the actual cost of security failure might do to the organization?

Control the conversation — and don't allow the technical to dominate what should be a *business* conversation about your firm's specific security risks and costs.

For example, you need to know which of your employees can use their iPads at the local Starbucks to log into your corporate database, what kind of information they can access, and how exposed to attack this makes your organization. You don't need to know if it's firewall or firefly technology protecting the corporate jewels as long as it does the job.

If your security conversations amount to nothing more than a list of product features designed to thwart some list-of-risks, then be concerned. And seek advice from a trusted security services partner.

CHECK OUT MORE OF TIM'S THINKING AT www.questsys.com/CEOBlog/

IT SECURITY MONITORING *(Cont. from p. 1)*

Indeed, as Cisco's *2014 Annual Security Report* confirms, most organizations, large and small, have already been compromised and don't even know it. Among the business networks analyzed by Cisco, 100% have traffic going to websites that host malware.

"Every organization is different," says Tim. "What works for one company may fail in another. But there are some security universals that every business should pay attention to."

Beginning with security policy

"Effective information security starts at the top — not necessarily in IT — and always begins with a strategy explicitly designed to protect business value," says Tim.

> "If your data has any 'street value,' someone somewhere will figure it out. And that puts even smaller organizations' data at risk."

"From this, you can derive a security policy so you'll know what data you have and how to protect it. You'll have rational rules about user access and privileges. You'll have procedures for handling incidents. You'll get your employees adequately trained in security awareness. And you'll have the means to evaluate how effective your IT security really is."

Needed: Continuous security monitoring

Next on Tim's list is an admonishment: "Resist the urge to believe your point security products will keep your data, apps and systems safe, because this simply is not true."

The problem: Disaggregated point and point-in-time solutions have not been designed to work together, and they can't respond to many of the advanced strategies and technologies now used in cyberattacks.

"If you can continuously monitor and manage information security, you can get real-time visibility into the behavior of devices, operating systems, services, applications, users, and so on," says Tim. "This speeds up attack time-to detection, helps spot previously unseen weaknesses and identifies attack patterns and contexts."

The right security monitoring/management capability should also be customizable. "If you don't have sufficient IT security staff," Tim advises, "find an experienced security services provider who can help you develop a security strategy and policy, a provider who knows how to determine precisely what your business needs are and how to implement your plan."

This will not only improve your overall security stance, it will help you control security costs."

Quest's Security Services:

Leading-edge, Proactive Security Capabilities You Can Trust

If today's IT security landscape seems so daunting that you'd rather just not have to think about it, you can be forgiven — right up 'til the moment your business suffers an incident.

That's when you'll discover the importance of a proactive, 24/7 real-time security monitoring and management capability operated by experienced, dedicated, trusted experts.

Bringing such capability to your enterprise is easier than you think, thanks to Quest's extensive array of IT and physical security services, which we'll combine and integrate in precisely the customized way your organization needs to achieve and maintain cost-effective defenses against breaches and hacks.

Start with one or more of our scans, assessments, and reviews, which can show you where you're vulnerable and what to do about it:

Quest's Security-Related Assessments, Scans & Reviews

- Security Discussion/Security for the Half-Day
- Firewall Review
- Application Security Scan
- Malware Assessment
- Physical Threat Vulnerability Review
- Video Surveillance Assessment

Quest's Security-Related Managed Services

- Security Posture Assessment
- Managed Security Intelligence Event Management
- Data Loss Prevention Solutions and Services
- Mobile Device Management
- Managed Unified Threat Management Services
- Enterprise Firewall Design and Management
- Intrusion Detection/Prevention
- Vulnerability Scanning
- Application Scanning
- Managed Antivirus Services
- Email Virus Protection/Spam Detection
- Managed Web Filtering
- Wireless Security
- Quest's Security Response Team (SRT)
- Computer Security Incident Response Planning and Management
- Computer Forensic Data Collection and Analysis
- Managed Network Services
- Client VPN Design
- Managed Site-to-Site VPN Service

Quest's Physical Security Services

- Video Surveillance as a Service
- Access Control
- The Quest Panic Button

Quest's security experts and Professional Services teams can help you keep your corporate security policy in tune with changing times and technologies. We're ready when you are to design, build, manage, and support everything you need for information, infrastructure, and physical security.

DID-YOU-KNOW?

Cyberattacks: A Matter of *When* ... Not *If*

Today's cyberattacks are sophisticated, well-funded, often relentless, and capable of causing major disruption to the companies they target. Here's a quick look at how exposures to security vulnerabilities and threats have ballooned between 2012 and 2013:

As cyberattacks grow more complex, so do organizations' exposures to vulnerabilities and threats

Increased exposure in 2013 to *vulnerabilities** from ...	
Mobile computing use	+45%
Social media use	+32%
Cloud computing use	+25%
Careless/unaware employees	+24%
Outdated information security controls/architecture	+18%
Unauthorized access (e.g., due to location of data)	+15%

* the possibility exists of being attacked or harmed; data based on actual incidents

Increased exposure in 2013 to *threats*** from ...	
Phishing	+32%
Malware (e.g., viruses, Trojan horses)	+31%
Spam	+29%
Cyberattacks disrupting/ defacing the organization	+20%
Fraud	+17%
Cyberattacks to steal financial data	+15%
Cyberattacks to steal intellectual property/data	+13%
Natural disasters	+10%
Espionage	+ 8%

** hostile action inflicted by actors in the external environment; data based on actual incidents

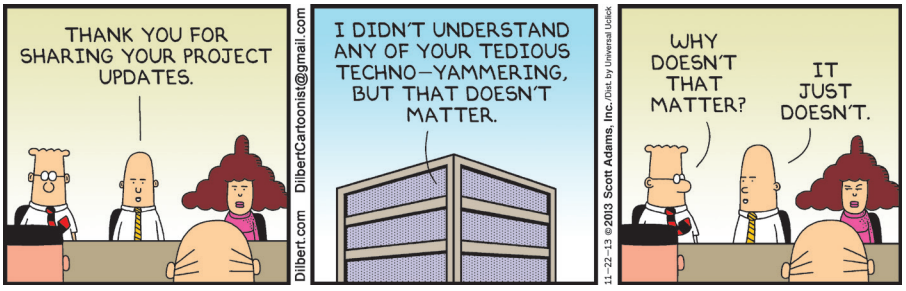
Source: *Under Cyber Attack - EY's Global Information Security Survey 2013*

What's New...
2014 Security Predictions: A Brave World of Blurred Boundaries

"It helps to be a little paranoid when it comes to computer security," notes security vendor Trend Micro's chief technology officer Raimund Genes in a recent paper* from the company that lays out eight security predictions for 2014:

1. As mobile banking services endure more man-in-the-middle (MitM) attacks, basic two-step verification will no longer suffice.
2. Cybercriminals will use more targeted-attack-style methodologies (e.g., open source research, customized spear phishing) along with multiple exploits.
3. Targeted attacks will employ more clickjacking and watering hole attacks, new exploits of choice, and attacks via mobile devices.
4. Expect one major data breach incident per month in 2014. Not surprising, given how easy (and cheap) it is for cybercriminals to buy malicious toolkits online (see #6 below).
5. Attacks that exploit vulnerabilities in widely used but unsupported software will intensify (e.g., Java 6, which is still run by 50% of Java users, and Windows XP, which still sits on 20% of PCs and claims an installed base of more than 300 million corporate computers).
6. Despite more funding and initiatives, the Deep Web — where the malicious can take advantage of darknet anonymity — will continue to challenge law enforcement, which lacks adequate protocols and personnel.
7. Exposure of state-sponsored monitoring activities last year has fostered broader security awareness — but also deep distrust of governments. A rethinking of where data should best be stored to keep it truly private will occur in 2014.
8. Widespread, large-scale Internet-of-Everything threats have not yet emerged, since these will require a "killer app" (appearing first, perhaps, in augmented reality devices like heads-up displays and drones). Instead, the new "easy target" of proof-of-concept attacks will focus on radio-frequency-enabled technologies (such as automatic identification systems) as well as gamers.

* http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-trend-micro-security-predictions-for-2014-and-beyond.pdf



DILBERT: © Scott Adams. Used by permission of Universal Uclick. All rights reserved.

FRIEND, FOLLOW, FIND QUEST

facebook.com/QuesTechUSA
twitter.com/QuesTechUSA
youtube.com/QuesTechUSA

IN THE MEDIA ROOM

VISIT QUEST CEO TIM BURKE'S BLOG
(www.questsys.com/CEOBlog/)

QUEST EXECUTIVE BRIEFS

Getting the Most from Cloud Computing (3-part series): Learn what it is and how it can help your business thrive (http://www.questsys.com/getMostCloud/).

10 Strategic Essentials for Boosting Business' IT Security: Key strategic security steps every organization should take (http://www.questsys.com/BoostITSecurity/).

Protecting Your Critical Business Data: The Data Loss Prevention Payoff: How data loss prevention (DLP) technology can protect corporate data from misuse, malicious or otherwise (http://www.questsys.com/PowerofDLP/).

NEWSLETTERS

Get current and back issues of our popular newsletter.
Manage your Newsletter subscription:
Let us know how you want your newsletter sent at http://www.questsys.com/SANpreference.aspx
Choose an emailed PDF or hard copy via USPS.

Quest STRATEGIC ADVISOR
Publisher: Tim Burke
Editor: Barbara Klide
Contact the editor at: barbara_klide@questsys.com