VOLUME VIII, NUMBER 3

Quest® STRATEGIC ADVISOR

www.questsys.com

Quest® | STRATEGY ADVISORY

Who's Watching Your Security *Right Now?*

Security is one of those things we tend to take for granted — until something goes wrong.

"You may not think much about the security implications of, say, deploying virtualized servers in your data center or allowing your people to use their own smartphones and tablets at work or on the road," says Quest President and CEO Tim Burke. "Yet each of these and other changes introduces new vulnerabilities."

And in response, you may bring in yet another point solution. If you're diligent about this, you may have dozens of these discrete, focused security products. But they're disconnected, unable to communicate — so, too often, though each might succeed at its narrow task, a breach happens anyway.

Is there a target on your back?

Meanwhile, the threat landscape is changing. Attackers are shifting from the random, everywhere-at-once release of malware to targeting specific organizations. The purposes vary — steal intellectual property or customer data, cover up fraud or leave a "logic bomb," demand ransom to allow access to data — and no one is exempt.

According to Symantec's *Internet Security Threat Report 2013,** small businesses have become the path of least resistance for attackers. In 2012, 50% of all targeted attacks were aimed at organizations with fewer than 2,500 employees — and 31% of targeted attacks took aim at companies with 250 employees or less.

"If you're operating a smaller business, you can no longer assume your smallness keeps you safe and secure," warns Tim.

"In fact, smaller enterprises are targeted precisely because too often their security tends to be less stringent," he says. "Attackers may decide to breach the weaker defenses of a small firm so they can work their way into the larger firms a small outfit does business with."

Add in the costs of not complying with expanding regulatory requirements — Sarbanes Oxley, GLBA, FISMA, HIPAA, PCI-DSS, NERC, CIP — and a security breach can have significant impact on your bottom line.

The good news: Security Intelligence Event Management

Because targeted attacks use a variety of vectors, such as malware-infected email, watering hole attacks, and zero-day vulnerabilities,

WHO'S WATCHING? *(Cont. on p. 2)*

THE BOTTOM LINE

To recognize attacks as early as possible, you need the ability to spot anomalies *in real time* — and that means gathering, integrating, and analyzing event data from all over your network.

* http://www.symantec.com/security_response/publications/threatreport.jsp

IN THIS ISSUE

WHO'S WATCHING?*(Cont. from p. 1)*

they can be difficult to detect. This makes quick recognition of anomalies very important.

"The ability to continuously monitor all activity in real time is becoming a necessity," says Tim. "Got a high number of failed logins to critical servers? You may be looking at a brute-force password attack. Notice an inappropriate use of protocols? Sensitive data may be exfiltrating. And that unusual Windows service you see running? That could be spyware."

> "The ability to continuously monitor all activity in real time is becoming a necessity."

Security Intelligence Event Management (SIEM) tools are designed to make sense of such discrete anomalies. SIEM enables you to gather and integrate data from security devices like firewalls, intrusion detection/prevention systems, and server security logs, then analyze it to identify issues and deal with them proactively.

Making easier work of SIEM

However, SIEM tools are complex and notoriously hard to implement and manage.

"SIEM is deeply valuable," Tim notes, "but it requires a good amount of integration, configuration, and ongoing maintenance. Too often, it takes the kind of time and expertise that businesses just don't have."

For many organizations, the best alternative is a managed service that provides SIEM capabilities — and the access to the specialized expertise essential to making it succeed.

Quest's managed SIEM offering enables data collection configuration, management, monitoring, and deployment on a wide variety of systems, thanks to a policy-driven, central-console event source management framework.

Raw log data is parsed, correlated, analyzed, and compiled so your event data is easy to understand and use. It's also easily searched and filtered, and Quest SIEM real-time reporting means you'll be able to see how your security and compliance posture changes over time, giving you a continuously complete picture of your environment.

"These days, it's important to be able to monitor your network for anything out of the norm without having to know exactly what you're seeing at the time," says Tim. "A managed SIEM service makes that both possible and affordable."

FROM TIM BURKE...

CEOs in the Crosshairs

When it comes to security breaches, CEOs stand in the crosshairs. More than their IT staffs, it's a CEO who'll take heat for a breach that exposes customer data or endangers relationships with business partners.

So, unlike plenty of other IT issues that don't require C-level attention, information security ranks right up there alongside financial issues as something with which CEOs need to be familiar. Yes, information security can be daunting, but so are financial statements — and CEOs have to sign off on those.

Where to start? Here are three questions every CEO should be able to answer: Do you know who your security expert is? Do you have a security policy? Do you understand how it's implemented, managed, enforced, monitored?

Getting answers to these sorts of general questions about how your company approaches its information security obligations is a good beginning — but your job isn't done yet. Like corporate financial issues, company information security requires more. In finance, that means an audit. I suggest you apply that same process to your information security.

A good security review will reveal any issues and also produce recommendations.

When it comes to information security, there are no guarantees, but exposing vulnerabilities and developing a plan to address them, can help keep your corporate data — and your bottom line — safe.

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

Quest's Security Services and Solutions:

For Security that Never Sleeps, Come to Quest

To be effective, your security needs to be layered, integrated, proactive, and well-managed. That's why Quest offers a full range of leading-edge security capabilities — including real-time Security Intelligence Event Management — that can be customized to your organization's unique requirements.

We'll deliver the capabilities you need in the ways that best suit you, whether that's Managed and/or Cloud Services via our remote 24/7 Network Operations Centers or via software, appliances, or services at your site.

Quest's security-related assessments

Don't know your security requirements? Don't worry. Our scans, assessments, and reviews can show you where you're vulnerable and what to do about it:

> 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-related Professional Services

Our security experts can help you keep your corporate security policy in tune with changing times and technologies as well as prepare you for audits, forensics, compliance analysis, and MasterCard/VISA certification processes.

We can also deploy and manage security-related projects, including real-time monitoring, management, and proactive intervention; mobile and wireless security; infrastructure and network security; intrusion detection/protection systems; and integration of Cloud, networking, and data storage with physical security solutions.

Quest can design, build, manage, and support everything you need for information, infrastructure, and physical security.

DID-YOU-KNOW?

Dangers of Web-Based Attacks Loom Large

In its *Internet Security Report 2013*, Symantec notes that web-based attacks increased by a third in 2012 over 2011.

Bad guys infiltrate legitimate websites, installing attack toolkits and malware payloads so that those visiting the site get infected.

"A hidden piece of JavaScript™ or a few lines of code linking to another website can install malware that is very difficult to detect," the Symantec report states. "It then checks the system of each visitor for browser or operating system vulnerabilities until it finds one that is likely to succeed and it uses that to install malware on the visitor's computer."

Such attacks depend on out-of-date software patches. This happens often with both consumer and employee devices. It also happens in businesses whose critical systems depend on older software versions, making upgrades to the latest secure versions problematic.

Readily available toolkits exploiting well-known vulnerabilities enable criminals to target millions of devices and find those open to infection. Little wonder that the most-exploited vulnerabilities are not the newest. Even so, says the Symantec report, the rate of discovery of vulnerabilities has only increased by 6%.

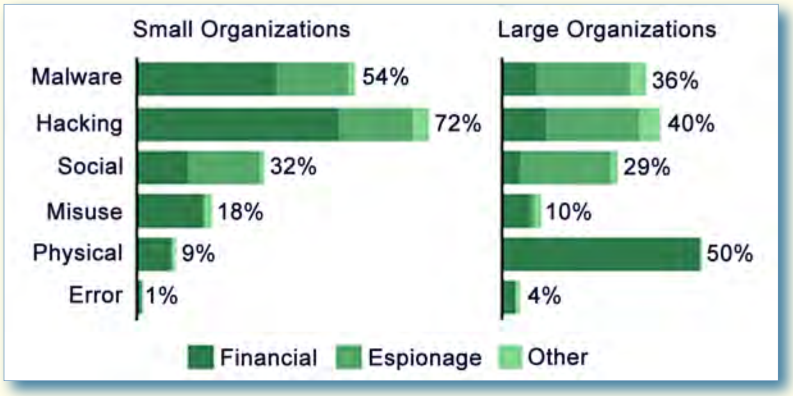
What's New...

A look at the attacks small businesses face ...

Verizon's *2013 Data Breach Investigations Report** takes a close look at what attackers are up to and how it impacts both large and small (fewer than 1,000 employees) enterprises. Here are a few highlights about discovered breaches:

> 78% of initial intrusions rated as low difficulty
> 75% were driven by financial motives
> 71% targeted user devices
> 69% were discovered by external parties
> 66% took months or more to discover.

The report identifies several threat action categories and tallies each by the attackers' motivations (financial, espionage, and/or other):



* http://www.verizonenterprise.com/DBIR/2013/

Quest® STRATEGIC ADVISOR

Publisher: Tim Burke
Editor: Barbara Klide

Contact the editor at
barbara_klide@questsys.com

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/)

THE QUEST YOUTUBE CHANNEL

(www.youtube.com/QuesTechUSA)
Master Your Disaster, parts 1-4
DR for the Day ... and much more

QUEST WEBSITE VIDEOS

(www.questsys.com/media.aspx)

Who We Are: Colleagues describe how Quest helped them.

Service Delivery Centers: They're why you can count on Quest.

Business Resumption Center Online Tour: Secure, seismically-stable 24x7 availability — Quest's BRC is the ultimate in disaster preparedness.

Business Continuity Planning/Disaster Recovery: More than 25% of businesses damaged from natural and/or man-made disasters never recover. Ensure your future.

DR for the Day®: Find out if you're ready.

Data Security: The FBI, security experts, and your peers on today's security issues and how Quest can help protect you.

Overview of our Infrastructure Services

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.

MY SECURITY SOFTWARE KEPT INSISTING THAT I DOWNLOAD CRITICAL UPDATES.
scottadams@aol.com
www.dilbert.com
I DIDN'T HAVE TIME TO DO ALL THAT, AND I COULDN'T RISK USING MY COMPUTER WITHOUT CRITICAL UPDATES. IT WAS A NO-WIN SITUATION.
8-9-08 © 2008 Scott Adams, Inc./Dist. by UFS, Inc.
DID YOU ACCOMPLISH ANYTHING THIS WEEK?
WHAT PART OF "NO-WIN" IS CONFUSING YOU?

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