Quest TECHNOLOGY MANAGEMENT

STRATEGIC ADVISOR

VOLUME XI, NUMBER 2

Cyber Security: Are You Prepared? Or Are You Prey?

"Cyber attacks and security breaches have grabbed plenty of headlines lately," observes Quest President and CEO Tim Burke, "but it can be hard to believe it'll happen to you. Until it does."

Today's increasingly sophisticated cyber criminals operate very much like any other enterprise — complete with management structure and quality control, sometimes even offering crimeware-as-a-service.

PricewaterhouseCoopers* notes that, globally, 32% of organizations have been impacted by cyber crime, which is now the world's second-most reported economic crime (behind asset misappropriation and catching up quickly).

Are you prey?

"If you don't know what's going on in your technology environment, if you don't stay on top of your security policies and who's enforcing them," says Burke, "then it's only a matter of time before you're prey."

Your necessary embrace of mobile, social, cloud computing, and the Internet of Things exposes your enterprise to an array of new threats, not least of which are those triggered by the unwittingly negligent behavior of well-intentioned employees.

Your infrastructure, industrial control systems, and intellectual property face advanced persistent threats possibly sneaked into position (sometimes using diversions like a DDoS attack) years before an incident reveals their presence.

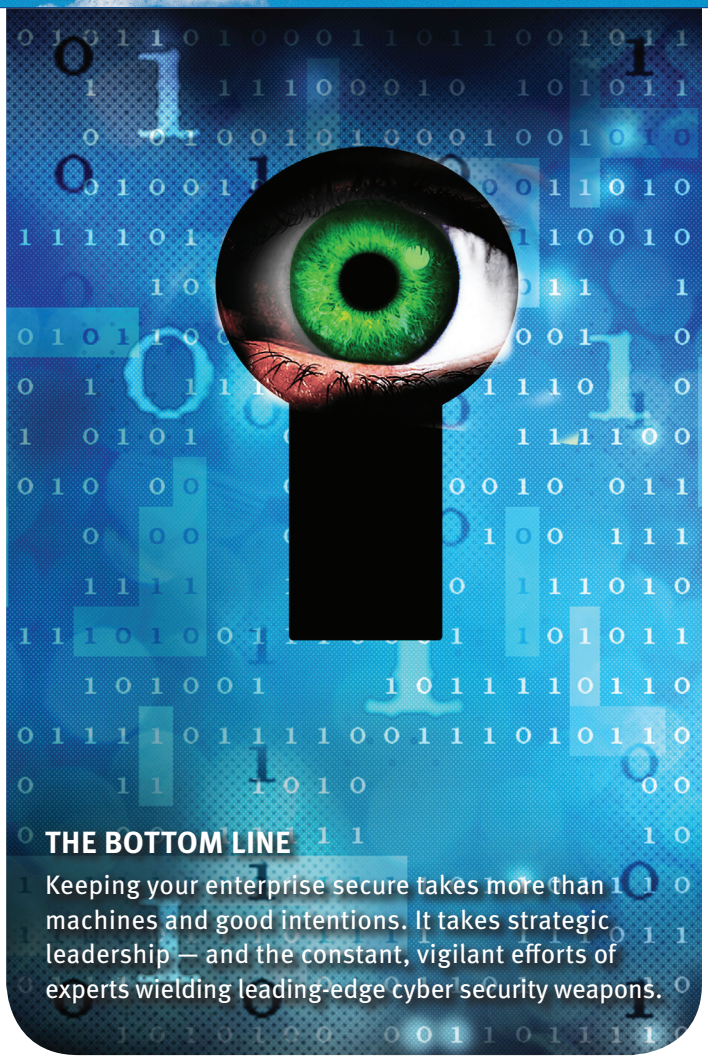
Your people are, perhaps, most vulnerable of all — to an ever-widening range of social engineering exploits that can lay your business bare. Example: spear phishing attacks that target C-suite executives.

And then there's ransomware, which typically encrypts files on an infected system and successfully denies access to the files and/or system functionality until a ransom is paid.

Needed: constant expert vigilance

"Hackers are very good at exploiting poor employee habits," Burke says. "But it's the boss's reactive approach to cyber security that can cost a business the most."

continued on page 2



THE BOTTOM LINE

Keeping your enterprise secure takes more than machines and good intentions. It takes strategic leadership — and the constant, vigilant efforts of experts wielding leading-edge cyber security weapons.

IN THIS ISSUE

Proactive cyber security is just an assessment away.

FROM TIM BURKE...

What's the Problem with Cyber Security?

Gartner estimates global spending on security will top $170 billion by 2020. As our page 1 article shows, that money must chase a fast-moving target.

Cyber criminals continually invent new hacks, new scams — and new business models. Yet, a report from 451 Research points to cyber security buying patterns dominated by investments in products that are, too often, aimed too narrowly at yesterday's cyber crimes.

So if, for instance, your security efforts consist mainly of deploying network and endpoint security products, you could be more vulnerable than you think.

I urge you to resist the temptation to believe that your cyber security issues will be solved as soon as someone sells you what sounds like the "right" product. Our experience indicates many are at risk because they lack a dedicated, forward-looking focus on security as part of business strategy.

No product — or layers of products — can compensate for a lack of strategy or a poorly-designed, roundly-ignored security policy or undertrained, overworked staff.

Our recommendation is to stop thinking of security as a bunch of products to install and promptly ignore. What you need is an all-encompassing cyber security strategy that drives your security policy, the solutions you deploy to enforce that policy, and the expertise required to stay ahead of the bad guys.

If you're unsure how to proceed, get help from a trusted cyber security advisor willing to pay attention to your unique needs.

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

CYBER SECURITY *(Cont. from p. 1)*

Lack of cyber security strategy and poor policy implementation, he notes, lurk behind many ransomware incidents.

If, for instance, you fail to keep your technology infrastructure up-to-date, you're extremely vulnerable. And datacenters with mixes of legacy hardware and software can be difficult — sometimes impossible — to protect.

Nor will throwing up layers of off-the-shelf appliances, even bleeding-edge ones, be sufficient to close the gaps, Burke says. "The security singularity is a long way off. Effective cyber security requires constant expert vigilance."

> "Security is a strategic issue. If you can't do it right yourself, get help."

That expertise is human and increasingly hard to come by, which likely accounts for why only 37% of organizations have a cyber incident response plan, and a mere 29% have an accurate inventory of their own data.*

"Security is a strategic issue," Burke emphasizes, "Protecting your business requires the proactive enforcement of basic cyber security hygiene. If you can't do it right yourself, get help."

Effective cloud and managed security services operated by experienced professionals are inexpensive, he points out, especially compared to what you can lose in a cyber attack.

Beginning with a security assessment

Burke says the move from a reactive to a proactive cyber security stance begins with a security assessment that covers your networks, servers, databases, applications, mobile environments, and even your physical security.

"The best way to know just how secure your cyber security really is," he explains, "is to bring in trusted experts to conduct a comprehensive security assessment."

Because today's technology environments have become so complex and dynamic, Burke advises against doing such an assessment yourself unless you have a large IT security staff.

"A security assessment done by an experienced professional," he says, "can measure and review the effectiveness of your security policies and procedures, expose your vulnerabilities before they're exploited by bad actors, and not only pinpoint what needs to be upgraded or redesigned but also offer multiple viable options for getting it done."

* Source: Global Economic Crime Survey 2016 [http://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf]

Quest Security Services:

Expert Cyber Security Services Designed Just for You

Quest offers cyber security services in customizable configurations that we can uniquely adapt to the security requirements of your technology environment.

Begin with a security assessment

Before you can deploy effective cyber security, you have to know what you need. Quest can help you find out via:

- Risk Management Workshop
- Security Policy Workshop
- Security Workshop
- Firewall Review
- Backup and Data Recovery Review
- Physical Security Assessment

Quest Managed Security Services

Delivered from our Network Operations Centers, our Managed Security Services are policy-driven, secure, compliance-focused, and feature simplified search, filtering, and reporting.

Our fully-monitored security information and event management (SIEM) and log management analytics underpin the real-time reporting and historical data you need for a comprehensive view of your security posture. Anomaly detection spots anything out of the norm on your network and recognizes new or unexpected trends/issues.

We can custom-configure a potent defense-in-depth tailored to your enterprise with our many services:

- Security policy and management
- Firewall management
- Enterprise anti-virus management
- Intrusion detection and protective response needs
- Enterprise management, performance & health management
- Security monitoring & management
- VPN management
- Business continuity, disaster recovery, restoral management & backups
- Security policy/audit/implementation
- On-site or remote network health monitoring
- Support/maintenance management
- Configuration, patch, and vulnerability testing & management
- Email threat management
- Computer forensics

Quest Data and Security Vulnerability Services

We offer a range of services focused on protecting your data:

- Encryption
- Automatic elimination of data on stolen or lost equipment
- Remote data destruction
- On demand vulnerability
- Assessment reporting
- Data security assessments
- Online backup or replication

Quest IP Video Surveillance Systems & Monitoring

Our infrastructure team can also manage, build, and support your IP video surveillance needs through assessment, design, implementation, 24x7 managed service support, and system maintenance.

DID-YOU-KNOW?

15 Ransomware Avoidance Tips

1. Use up-to-date anti-malware with proactive protections
2. Keep your firewall turned on 24x7 and use it to segment your corporate network
3. Scan compressed and archived files
4. Back up files (and encrypt them) at least daily
5. Make sure all your software is patched and up to date
6. Configure webmail servers to block attachments with certain extensions (.exe, .vbs, .scr)
7. Block known-malicious Tor IP addresses
8. Turn on Show File Extensions
9. Disable macros, ActiveX, AutoPlay, file sharing
10. Consider disabling vssadmin.exe, Windows Script Host, Windows PowerShell, remote services
11. Install a browser add-on to block popups
12. Consider installing Microsoft Office viewers
13. Switch off unused wireless connections
14. Prevent executable files from running from specific locations (e.g., ProgramData, AppData, Temp)
15. Train employees to:
    - Verify all email senders, double-check for spam
    - Never click on links in emails/attachments from strangers; be wary of any unsolicited attachments
    - Use strong passwords
    - Minimize administrator login time
    - Turn off the Internet connection immediately upon spotting a suspicious process

What's New...

More Awards for Quest

In 2016, Quest continues to be recognized for excellence in technical expertise and innovation in managed services delivery.

CRN® 2016 Tech Elite 250 list

Quest has been named to the CRN® 2016 Tech Elite 250 list in recognition of its deep technical expertise and premier certifications.

The Tech Elite 250 honors an exclusive group of North American IT solution providers earning the highest number of advanced technical certifications from leading technology vendors.

CRN's parent firm, The Channel Company, conducts research annually to identify the most customer–beneficial technical certifications in the North American IT channel. All Tech Elite 250 technology companies have obtained these elite designations, empowering them to deliver premium products, services, and support to channel customers.

2016 MSP 500 list in the MSP Elite 150 category

Shortly before it named Quest to its 2016 Tech Elite 250 list, CRN named Quest to its 2016 Managed Service Provider (MSP) 500 list in the MSP Elite 150 category.

This means Quest has been recognized as one of the nation's leading large datacenter-focused solution providers offering professional services on-premise as well as off-premise and excelling at developing cutting-edge approaches to delivering managed services.

"We believe," says Quest President and CEO Tim Burke, "that it's important for clients to be able to choose the degree of control they maintain over their IT services. We help them formulate their own overall management environment, which can, if a client chooses, span servers, networks, data storage systems, security, and DR/BCP/Business Resumption planning and testing.

"It's elegantly simple," says Burke. "Quest supplies the technology expertise exactly how you need it so you can concentrate on your core business."

FIND, FRIEND, FOLLOW QUEST

facebook.com/QuesTechUSA
twitter.com/QuesTechUSA
youtube.com/QuesTechUSA
linkedin.com/company/252386?trk=tyah

QUEST PLAYBOOK

What we offer:
http://www.questsys.com/ePlaybook

QUEST ASSESSMENT SERVICES

Test drive our services, evaluate our expertise.

For a complete listing, go to: http://www.questsys.com/assessment-services.aspx

Disaster Recovery Workshop
http://www.questsys.com/disaster-recovery-services/disaster-recovery-workshop-video.aspx

Security Workshop
http://www.questsys.com/security-workshop-video.aspx

Cloud Workshop
http://www.questsys.com/cloud-assessment/

IN THE MEDIA ROOM

VISIT QUEST CEO TIM BURKE'S BLOG

(www.questsys.com/CEOBlog/)

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