Straight Talk from the Corner Office

February 2014

5 Ways to Keep Your Business off the Cybercrime Casualty List

Welcome again to *Straight Talk*, one of the ways Coranet shares perspectives on important issues and opportunities in business communications.

Our fall “Spotlight” focused on the significant -- *and growing* -- threat that cybercrime represents to all businesses, big and small. Since then, the seriousness of these cyber attacks has been further driven home with the brazen theft of personal financial information from major retailers, such as Target, Neiman Marcus and Michaels.

With security-related financial losses for U.S. companies estimated to easily exceed a billion dollars this year, it's clear that cybercrime prevention warrants serious attention by business owners and executives. Thankfully, this message appears to be hitting home. In the 2013 annual survey of over 3,000 IT leaders by global research firm *TechTarget*, security and disaster recovery initiatives represented three of the five top spending priorities.

Top 5 IT Priorities

#1 Data Protection
#2 Server Virtualization
#3 Network Security
#4 Disaster Recovery
#5 Business Intelligence/Analytics

TechTarget 2013 IT Priorities Survey, n= 3,282

For this winter issue of *Straight Talk*, we’ll focus on concrete steps you can take to decrease the likelihood that your company will fall prey to cybercrime.

An Essential Business Security Checklist

In a comprehensive study released in January on the current state of business security, Cisco Systems delivered a blunt assessment that, at best, most companies had a highly fragmented approach to security that fell way short of providing any effective protection.

To avoid this pitfall, a comprehensive and integrated approach for your firm's business security is definitely the way to go.

1) First Things First: *A Reality-based Plan*

The best way to help ensure effective protection for your business is to start with a thorough security plan. Good planning addresses two key areas: **assessment** of your business infrastructure, applications and policies, and development of specific **strategies** that address the security vulnerabilities uncovered during the assessment.

Even for companies that are highly attuned to the importance of business security, it's very likely that vulnerabilities exist in their systems, devices and business processes that provide a ready-to-exploit path for cyber attack. A rigorous assessment will systematically inspect and evaluate the susceptibility of your end-to-end network to external as well as internal intrusion. A comprehensive approach is key, so be sure that all network components are assessed, including firewalls, routers, email and web servers, desktop phones, mobile devices, remote access mechanisms such as VPNs, and any existing intrusion detection and prevention systems.

At its most basic level, a security strategy should leverage the findings from the assessment to achieve three desired outcomes:

- **Data confidentiality =** business information remains restricted to authorized users
- **Data availability =** business data is readily accessible when and wherever needed
- **Data integrity =** informational assets are protected against unauthorized alteration or deletion

When considering data confidentiality, make sure to include the full range of information that needs protection -- from highly restricted company financials and business plans, to unfiltered employee-only blogs and internal social media sites. Companies facing regulatory oversight also need to address the security implications of compliance mandates such as Sarbanes–Oxley or HIPAA.

There are two key points to keep in mind when it comes to developing effective strategies to minimize business risk. The first is **expertise**. As we discussed in the last Spotlight, cyber security is a fast-moving game of cat and mouse, with "lone wolf" attacks increasingly being supplanted by larger-scale criminal efforts. Ensure that the resources you commit to the assessment and strategy formulation phases are experienced and up-to-date on the latest -- *as well as emerging* -- forms of cybercrime tactics and threats.

The second key point is **frequency**. Security threats are constantly evolving and are becoming more sophisticated and difficult to detect. Assessments are *definitely not* a one-time event. Make sure you make provisions to re-assess your company's security profile on a regular basis -- *at minimum annually* -- and adjust your strategies accordingly.

2) Where the Rubber Meets the Road: *Implementation of Security Safeguards, Policies and Controls*

With a well-executed assessment and strategy, you have a solid basis for a security blueprint that details the specific actions needed to protect your informational assets while also ensuring that you are well-prepared.

However, security safeguards go far beyond deployment of anti-virus software at the desktop, and extend into the foundational capabilities of your network. Key among network-level safeguards are **identity management** and **access control** that allow your administrators to register end users and grant them permission to access specific data, applications and services. In addition to ensuring tight user authentication, a best practices approach would also involve conducting active monitoring of key applications and data stores to look for suspicious patterns that could signal employee misuse.

In addition, your action plan should extend beyond prevention to include an effective response capability should a cyber attack be successful. Your company needs to have a formal plan in place to determine the extent of the intrusion, contain the damage, and restore normal business functioning as rapidly as possible.

Just as in the assessment and strategy phases, the implementation of safeguards is another area where expertise is extremely important. Make sure your resources have the necessary skills to not only fortify the security of the company's infrastructure, but also to address the vulnerabilities in your business processes and operational procedures.

3) Two Areas of Increasing Vulnerability: *Mobility and Cloud*

The rapid expansion of bring-your-own-device and bring-your-own-application behavior among employees wanting to use non-sanctioned technology in the workplace represents a genuine and growing threat to business security. Increasingly, mobile devices are becoming the target of choice for cyber criminals; largely because they can be used to access corporate networks remotely and often lack the encryption safeguards that are standard with VPNs and wireless LANs. Similarly, the growing use of cloud-based Software as Service solutions opens up a whole new set of security concerns, ranging from hacker penetration of joint tenancy servers to credential hijacking.

4) The Absolute Need for On-going Intrusion Testing

In addition to conducting periodic capacity testing to ensure that your network has adequate bandwidth to handle ever-increasing data loads, it is just as important to regularly stress test your network's ability to withstand attack. Bottom line, there is no substitute for regularly scheduled intrusion testing -- *both external and internal* -- to discover any weaknesses in your security defenses before the cyber criminals do.

5) Business Security is More Than a Secure Network

Although it may seem somewhat mundane compared to combating high-tech cybercrime, don't neglect the many elements of physical security that also protect your company. Examples of these types of safeguards include establishing controlled building entry/exit points, situating essential servers in secure areas with video monitoring, maintaining up-to-date disaster recovery plans, and ensuring that fire suppression and uninterrupted power systems are regularly tested and are always fully operational. These contribute to and enhance your security defenses and business resiliency.

A few final thoughts...

Coranet's work with clients over the years to help them fortify their security defenses has underscored several key learnings.

First, establishing and maintaining the security of your company is serious business and warrants the personal attention and involvement of senior leadership.

Secondly, even when IT budgets are under heavy pressure, resist efforts to cut back on essential security spending.

Lastly, our experience strongly suggests that a holistic view which embeds security in every aspect of daily operations -- *not just the network* -- is the most effective approach to protect your business.

Thank you for joining me in this look at ways to reduce your company’s risk of falling prey to cybercrime. If you have any comments or questions, please reach us at questions@coranet.com.

Margaret