BRIEF:

Information Security: The Seven Signs Your Business May Be at Risk

Our ever increasing reliance on the internet is creating new challenges and threats that force organizations to continually rethink their protection measures. The dangers posed by hackers, malware and poorly constructed security procedures are real and the costs of failure can be catastrophic for any business. Organizations that understand those risks (and the warning signs of security breaches) will be better prepared to address their own specific system vulnerabilities.

TeamLogicIT®
Your Technology Advisor

The most costly problems are often the ones you don’t see and can’t predict. That can apply to the plumbing and electrical service in our homes, or the drunk driver coming at you just a few miles down the road. It is truly hard to comprehend how much damage a potential problem can cause until it occurs.

The Cost (and Value) of Information Access

That same rule applies to today’s technologies. As the information age matures, organizations (and individuals) are putting an increasing amount of trust in the Internet. “Accessibility” and “ease of operation” are common themes as more and more companies charge full speed ahead, attempting to leverage the most value from their websites, social media and mobile devices. As we rapidly advance in this new online paradigm, the push to connect virtually every person and business to the internet continues to grow exponentially each year—with no end in sight.

Of course, that level of accessibility comes at a cost. For every new user or access point, there has to be a corresponding protection measure. Each business must create its own unique system that balances the convenience of its employees and customers with strong security policies. Data and network protection must be a top priority, no matter how big or small they are or what line of business they conduct. Hackers and spammers are non-discriminatory—they take advantage of any opening and can significantly damage the network, infrastructure and reputation of any organization.

> *“75% of companies say IT risks impact customer satisfaction and brand reputation.”*
>
> – IBM statistics (http://www-935.ibm.com/services/us/en/it-services/data-breach/data-breach-statistics.html

The Cost of Failure

While some of the costs associated with these attacks are never published due to confidentiality and ongoing protection concerns, the estimates are staggering. In 2013, research conducted by the Ponemon Institute put a price tag on an average malicious security breach of $840,000! Litigation costs could easily push that number much higher and, if the organization was shown not to have followed the proper regulatory or industry compliance measures, the resulting fines could also be quite substantial.

The well-publicized Target data breach demonstrates the worst-case scenario, as approximately 110 million customer records were stolen during the most profitable time of the year for retailers. It will likely take years to calculate the full cost of this security failure. After all the lawsuits run their course and each of the numerous compliance fines are tallied, experts suggest the price tag will easily top $1 billion.

Businesses that become victims of cybercrime often don't report it to avoid the negative publicity and the effects it can have on their clientele and future earning potential. Unfortunately, that strategy frequently backfires and ends up damaging their reputation and bank accounts to an even greater extent.

Take the case of Maricopa Community College District, which recently notified almost 2 1/2 million of its current and former students, vendors and employees that their personal information may have been compromised. There was significant evidence directors knew about a breach in their data system for months, leaving the names, birth dates, Social Security numbers and bank account information for all those individuals unprotected. While the district's board of directors budgeted millions of dollars to boost security measures and an additional $7 million to notify all affected parties, the directors' negligence could substantially increase the cost of this preventable incident.

As Technology Advances, Protection Must Follow

If securing confidential business and client data were our only concern, the quick and easy solution would be to completely lock down all external communication points. Of course, in today's internet-driven society with increasing dependence on cloud and mobility solutions, that's simply not an option. The web drives business applications and gives employees and customers access to the information they need to make informed decisions. They want and, in many cases, need to be able to log on from anywhere, using virtually any device available.

> *"'Password1' is still the most common password used by global businesses. Of three million user passwords analyzed, 50% are using the bare minimum."*
>
> – The 2013 Trustwave Global Security Report

Based on all the advantages they bring to businesses and their workforce, the insatiable demand for Cloud computing and mobility services should not be expected to diminish. Each solution gives employees greater flexibility and can considerably improve an organization's sales and business development opportunities. In order to gain the benefits of cloud and mobility solutions, businesses must implement their own unique policies and security measures to protect their infrastructure and data. With greater access comes greater responsibility—for the organization and its employees.

Many information lapses originate from inside an organization. While 41% of businesses that experience a data breach place the blame on malicious attacks, 33% are attributed to employee negligence and 26% are simply "system glitches," according to the Poneman Institute. External security threats are a constant concern for every organization, but with the proper procedures and effective monitoring processes in place, many internal gaps can be managed or eliminated. Effective password and device management policies are just as crucial as updating the security software or services.

Your Business May Already Be Affected

Encryption, malware protection and multi-factor authentication should be mandated for all PCs and mobility devices. Email and other communications systems, such as instant messaging and teleconference programs should be constantly monitored for intrusions and unusual activities.

> *“In 2011 RSA, a major technology company, was hacked all when an employee responded to a phishing attempt. This is a company whose whole business was security, and fell victim to what hackers know, ‘No matter how secure a target the user is always the weakest link.’”*
>
> – Jim Guckin (http://www.jimguckin.com/about/)

Look for these 7 warning signs that your network and/or data systems have been corrupted by viruses or other malware:

- PCs, laptops, servers and other computing devices begin to slow, freeze or shut down on their own (crash).
- Co-workers, business contacts or friends report receiving spam messages from someone using a company email address
- Computer systems make processing sounds continually, even when not being used
- Web browsers switch automatically to other sites or search engines
- Unusual pop-up windows appear (even when not connected to a wired or wireless network).
- Error messages multiply and cannot be resolved
- Data backup processes fail, improperly save files or generate error messages

The Key Indicator

What is the single, biggest warning sign your security systems may be compromised? When you have no record or indication that every computer, server and mobile device is adequately protected, the level of exposure is simply incalculable. Information security is a constant struggle for many organizations; staying a step ahead of the latest wave of threats by continually updating defenses and strengthening employee best practices. Companies that fail to take those threats seriously often pay a high price with the resulting lawsuits and regulatory compliance fines, as well as lost revenue.

Finding that balance between network access and information security is a critical objective for every business, but it takes the right mix of technical expertise and industry knowledge that few organizations possess. That’s why many organizations, even those with their own IT departments, bring in third-party specialists who can identify protection issues and design solutions that address every existing and potential gap. Hiring a team of employees with those advanced skills may be impractical from an economic perspective, so finding a qualified outsource partner would be a much more valuable option.

That professional expertise is what managed service providers can bring to your organization. They can proactively monitor and adjust your company's security systems to counter the latest threat, and neutralize potential threats before they negatively affect network performance or compromise your data. If you're unsure of the current protection status of your business look to managed services professionals who will design, implement and support your long-term service needs. It will surely be the best data protection investment you ever make.

Sources Cited

2013 Cost of Data Breach Study: Global Analysis; Ponemon Institute, LLC; May, 2013
http://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf

"Target, Security Auditor Trustwave are Sued Over Data Breach"; Reuters, March 26, 2014
http://www.reuters.com/article/2014/03/26/us-target-trustwave-lawsuit-idUSBREA2P0B020140326

"California Business Scores Settlement in Thorny Cybercrime Case"; PCWorld, June 25, 2012
http://www.pcworld.com/article/258310/california_business_scores_settlement_in_thorny_cybercrime_case.html

"Maricopa Community Colleges Notifies 2.5M after Data Security Breach"; Phoenix Business Journal, Nov 27, 2013
http://www.bizjournals.com/phoenix/news/2013/11/27/mcccd-notifies-25m-about-exposed.html?page=all

For help with your IT security, contact your local TeamLogic IT office.

TeamLogic IT is a national provider of advanced IT management services for businesses. With locations across the U.S., TeamLogic IT provides managed services, computer consulting and support services focused on helping companies minimize downtime and improve productivity. TeamLogic IT helps businesses compete better through the effective use of information technology.