KONICA MINOLTA

Giving Shape to Ideas

Four Keys to Protecting Your Business

security

KONICA MINOLTA

Giving Shape to Ideas

Four Keys to Protecting Your Business

security

Table of Contents

Introduction

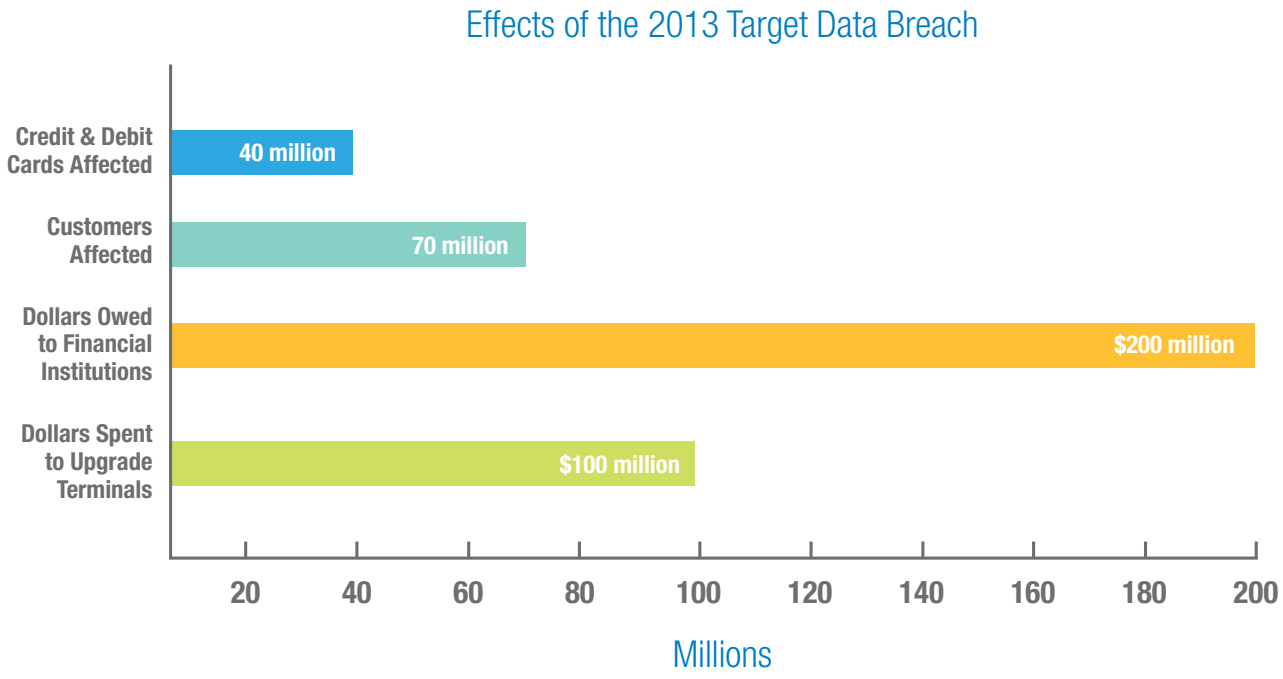
Problem. **As companies grow, it is easy to miss technology changes** that can expose your business to vulnerabilities. No business is immune. For example, the Target data breach affected 40 million debit and credit cards and 70 million customer records.

Hackers used credentials from Target's HVAC company to upload malware into the security and payment systems. As a result of the breach, Target stock dropped by 46 percent year-over-year in the fourth quarter of 2013. The cost of reissuing credit and debit cards that were stolen in the breach racked up a bill of approximately $200 million to credit unions and community banks. Target is now spending $100 million to upgrade their terminals. Possibly the biggest casualty of all was Target's reputation; a hole they are still climbing out of to this day. Every business should take this as a warning shot that protecting your business against breaches is not a "set it and forget it" situation.

The breach at Target is just one example of many that took place in 2013. In October of that year, Adobe announced they had been the victim of a breach that affected millions of users. The compromised data included profile information and, more importantly, credit card information. A large file was uploaded to AnonNews.org that appeared to include more than 150 million usernames and hashed password pairs taken from Adobe. The theft also included source code for Adobe's Acrobat, ColdFusion, and Photoshop products. The data was discovered on a server used by the same group believed to have hacked into LexisNexis and Dun & Bradstreet earlier in the year.

It is important to remember that businesses are targeted at all levels. It is not just the Adobes and Targets of the world that are experiencing these breaches. According to a July 2014 article by Forbes, SMBs are key prey for hackers. In 2013, SMBs collectively made up more than half of all targeted attacks at 61 percent – up from 50 percent in 2012 – with medium-sized (2,500+ employees) businesses seeing the largest surge.

These ongoing data breaches are proof that this problem is only getting more serious and widespread.There are, however, a number of steps a business can take today to help protect not just their data, but their entire network.



1 Key One: Build a Security Plan

Protect.

Building a security plan is the first, and some would say the most important step in protecting a business network. This should be a methodical process that includes the IT team and key business stakeholders. Businesses need to not only understand current security trends in the industry; they need to understand the current state of security within their own data center. Building a plan will identify current security lapses so the team can create a comprehensive approach.

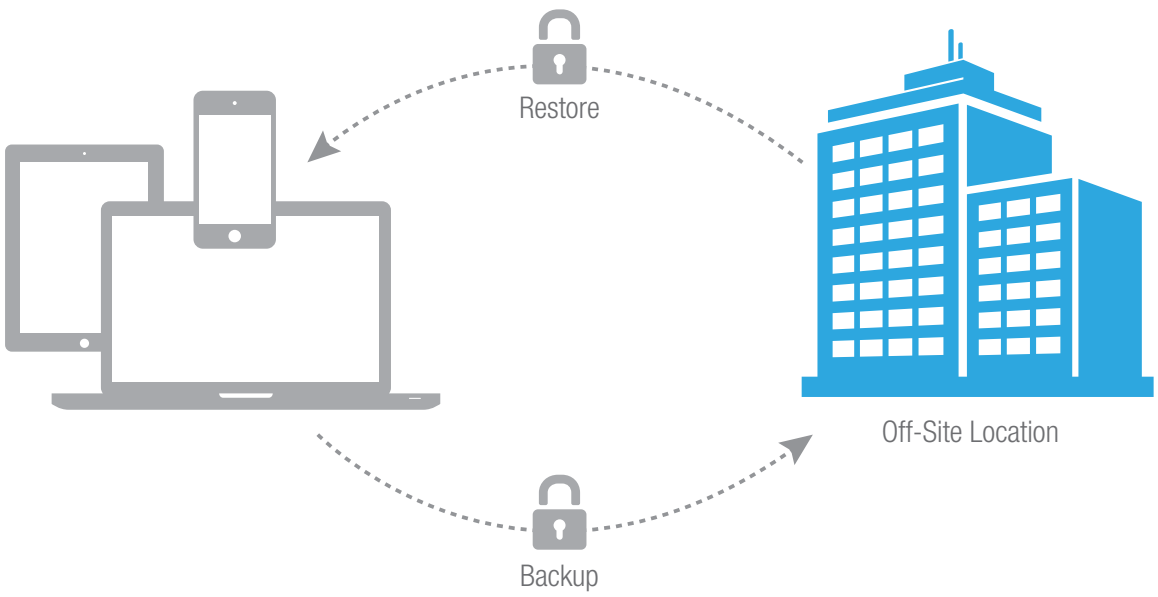
There are several steps involved with building a security plan. That plan should start with a discussion to acquire answers for the following questions:

Current Policies
A complete assessment of IT and security policies should take place. A security plan will cover many areas and there will be policies around each area like Acceptable Use, Passwords, Data Access, Backup and Recovery and many others. Policies should be reviewed on a regular basis to make sure they are current with the business' plans and goals.

Regulations
If the business is in a regulated industry, such as finance or healthcare, there may be additional requirements to keeping data secure and available for industry audits. It is always a good idea to speak with an industry expert, whether it is an employee or an industry official, to confirm all requirements are met.

Physical Structure
Nothing should be overlooked when building a security plan. Server rooms and data centers should be off limits to the majority of business personnel. Do the server room doors have security card access or programmable keypad door locks? What about an independent air conditioning system? Is there proper power protection with battery backup or even a backup generator? Is there proper fire suppression? These are all important parts of protecting a business. Look at the physical space with a critical eye. Everything from key cards for all employees to gain access to the building, authorized access to server rooms and proper power is important to protect a business.

Device and Software Inventory
Every device from mobile phones to servers should be part of a complete inventory. This will allow the business to understand the complete scope of their environment and the devices, software and systems that have to be part of a security plan. Include hardware configuration, installed business software and current security patch levels. This will identify if any critical patches have been missed or are not installing properly. While this could be a daunting process for a company with thousands of devices, it is an important step. For example, if it is simply not possible to inventory and check each mobile phone, consider checking at least the mobile devices of top and C-level management as well as the IT team. Those individuals are probably the most likely to fully utilize their mobile devices for business which could put them at greatest risk.



Strategy. **Once the fact-finding portion of the discussion is complete,** the team needs to take that information and begin to build the actual plan. Just like the initial research, the process must be comprehensive and the plan should be by the IT team and key stakeholders. Key points to remember should include:

Physical Servers
Develop a written backup and recovery plan. It should include the ability to restore from an image with confirmed and tested recovery points. It is crucial to remember that copies of the backup are kept at off-site locations in order to protect against a catastrophic failure.

Virtual Servers
Virtualization provides some wonderful benefits from an IT management standpoint, but also from a financial standpoint. However, just like their physical server counterparts, they still require a thoughtful plan for management and security. This should include monitoring and reporting on backup and replication, fault tolerant design and carefully planned capacity implementation.

End-Users Computers
Make sure every time a new computer is imaged it includes local endpoint protection software (antivirus, antimalware) set to auto-update to keep protection strong. Implement usage policies regarding internet usage, email usage, installing software, downloading attachments and the like. Human error is a large part of security breaches. If possible, consider desktop virtualization or thin client computing. These options provide both a flexible and more secure solution for end user access.

Employee Security Training
Part of any successful security plan includes employee training. Employees should be trained on the policies and procedures implemented by the company as well as best practices for email usage, internet usage, handling corporate data and any compliance related requirements. As company policies change or new one are instituted, employees will need to be trained on the changes.

Other Devices/
Bring Your Own Device (BYOD)
While BYOD is becoming a popular solution for businesses, there are also some inherent risks. As the device is not owned by the company, it can be difficult to manage and enforce security policies. Top concerns for BYOD deployment are routinely related to security. It is thought that approximately 22 percent of the total number of mobile devices produced will be lost or stolen during their lifetime, and over 50 percent of these will never be recovered. Will that device contain your valuable business data? As a result, it is important to consider application risks, password strength and possible encryption, as well as remote wiping for lost or stolen hardware.

2 Key Two: Implement Your Security Plan

Apply.

In its 2013 global data breach study, the Ponemon Institute reported that data breaches experienced by U.S. companies continue to be the second most expensive in the world at $188 per record. The study also reported that U.S. companies had the second greatest number of exposed or compromised records per breach at 28,765, resulting in an average total organizational cost of more than $5.4 million per data breach. By beginning the implementation phase of the newly established security plan, the team is taking an important step forward in preventing data breaches.

A good place to start with the implementation process is to hold a company meeting. This will serve a dual-purpose. First, it will communicate to all employees that the implementation of a new security plan, and/or revised policy, is underway. It gives them the opportunity to ask questions and really feel they are part of the bigger plan. Second, it will be a great opportunity to provide employees with important security training. The session need not be long; it just needs to talk about how to create strong passwords, identify questionable email attachments and avoid potentially troublesome websites. It is worth mentioning to them that they can take some of these work-related security ideas and apply them to their home computing as well! Once employees understand how the protection plan will work and how they can help keep the network secure, the more diligent they will be moving forward.

As mentioned previously, it is important to document all the agreed-upon policies, procedures and installation information identified in the first step and then distribute the documentation to all interested parties. This document should always be on hand in a centralized location, in case sections of the protection plan require an update, or disaster recovery plans need to be put into action. Have employees acknowledge in writing that they have reviewed the policies and understand them.

When it comes to starting the physical work, it is a good idea to start with making sure images of servers and desktop configurations should be updated on a regular basis. In case an emergency recovery is required, a desktop image a few months old is more than likely missing critical security updates. This means it will take additional time for the IT team to update each unit individually to keep it on par with all other parts of the overall protection plan.

Responsibility.

The selected endpoint protection software should be installed on all computers, servers and mobile devices. This software should be updated on an ongoing basis in order to keep protection at a high level. A minimum of two IT team members (for redundancy purposes) should remain active on the email notification list in order to receive notices of critical updates and alerts. It is not uncommon to have "emergency" patch alerts to plug security holes against a recent threat. By staying up to date on security best practices and current threat news, the software will be kept current and the network will remain protected.

Regardless of the size of a business, a solid firewall is a key part of keeping networked computers and business data safe and secure. A firewall serves two main purposes. It can filter what traffic comes into the network and it can control what users on the network may send out of the network. Just like all the other parts of the security plan, it is one piece of a larger methodology. The specific settings for the firewall will vary based on the type of other security-related processes in place and the business needs.

According to a recent study, in Q2 the percentage of spam in total email traffic increased by 4.2% from the first quarter of 2013 and came to 70.7%. The percentage of phishing emails in global mail traffic totaled 0.0024%. Malicious attachments were detected in 2.3% of all email.

Quite possibly the biggest variable when it comes to a business protection plan is regarding mobile devices. According to a 2013 global security study, mobile malware has exploded by 400 percent over 2012. Additionally, on average, today's employee utilizes three different devices for work-related tasks – and they all require security and data protection. One of the biggest potential threats is when an employee uses a public network. Whether at the airport or the coffee shop, the potential for malware and other threats are ever present. When implementing the mobile device portion of the plan, especially in a BYOD model, it is a good idea to sit down individually with each employee that utilizes mobile technology to conduct business and review the new security policy and how it directly affects mobile devices. These employees may not even be aware of all the security holes that exist in today's apps and connection points. One of the biggest stories this year was the far reach of the NSA. One of their "entry points" to private mobile devices? An unlikely popular app – the game Angry Birds. As soon as a player opened up the game and began playing, algorithms within the game's code relayed their age, sex and other information to intelligence agencies. This is according to documents leaked from GCHQ (Government Communications Headquarters), which revealed how it and the NSA had been working on ways to tap into mobile devices and collect data through commonly-used apps. In addition to Angry Birds, other apps that fell prey to government agencies included Google Maps, Facebook, Twitter and LinkedIn.

3 Key Three: Ongoing Protection

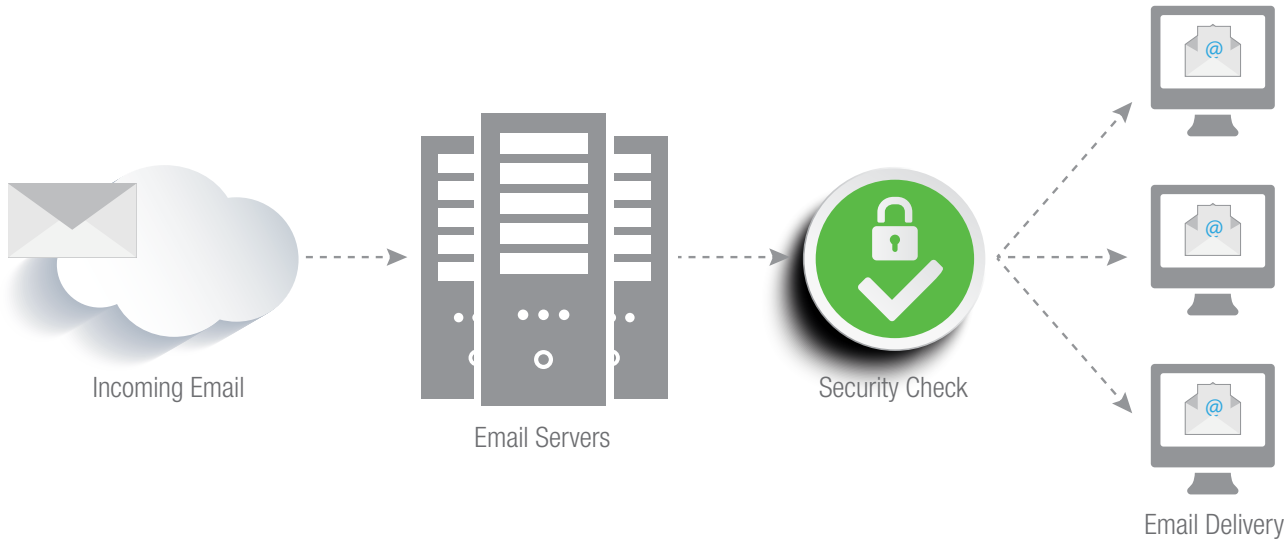
Regulate. **Once the security plan is in place, it doesn't mean that the job is done.** In all reality, it is just the beginning. As mentioned previously, business protection is not a "set it and forget it" type of situation. Protection requires ongoing audits, reviews and updates in order to keep a network in top shape and data completely protected.

The IT team should regularly conduct security tests to check on software updates for both employee computers and servers. The team also needs to stay apprised of security-related news and best practices. It is a good idea to have IT members participate in security conferences to understand all the nuances and latest technology related to industry best practices in order to prevent digital attacks. Spot checks on desktops are also a good idea to make sure automatic updates are truly taking place. Computers of employees that work with proprietary data should be checked most often.

According to research by Verizon, the largest malware action within cyber-espionage was related to email attachments (78 percent). This is further proof that email virus updates, spam filters and email encryption and continuity should have regular reviews and tests. Email archives should also have ongoing tests conducted to make sure they can have a recovery completed without issue. If there is an issue recovering an email archive, it should be investigated and rectified immediately.

Content filtering often receives negative press as a "big brother" approach to limited information access. However, it is really an effective way to protect business hardware from reaching websites that may contain malware which could wreak havoc on a business' network, and control the use of non-productive Internet usage. It is important, however, that the business share with employees that content filtering will be used to protect the network and that it is included in written policies. If not, it may have an "Orwellian-effect" on employees.

Finally, make sure to follow all documented backup and recovery procedures and, just like with email archives, test the backups periodically to ensure they are valid. It is also a good idea to keep a "backup to the backup" to be completely covered in the case of a major catastrophic event.



4 Key Four: The Cloud

45% of participants have moved past the pilot stage of their cloud implementation.

32% have a formal cloud computing plan.

Backup.

The cloud has been continuously gaining ground in recent years as a safe alternative for data storage, email management, backups and more. In a cloud environment, instead of the local IT team charged with maintaining servers in the business location, they work in concert with the cloud service provider to complete these tasks.

The servers are physically located at the cloud service provider's location and can handle running backups, and applying software patches and the like. This approach hands over the management of the physical servers and network infrastructure to the cloud provider, ultimately offering the business a more secure and streamlined environment. A major part of the day-to-day activities of the employees of the cloud provider is to ensure the servers in their charge are completely protected.

As the cloud servers are off-site, it makes the location completely independent, providing the most agile solution for businesses today. If there is a catastrophic disaster and the primary business location is not available, the users can easily go to a different locale and access the data so work can continue with minimal interruption. The cloud service provider keeps the hardware up to date and well protected against malware, viruses, etc. This includes the ability to provide hosted email services in order to gain top-level email security; arguably the most important line of defense against malware. They can also handle backup and scale resources up or down as business needs change.

Cloud solutions are a real and viable option for business protection today. According to a new study, 45 percent of participants have moved past the pilot stage of their cloud implementation and 32 percent have a formal cloud computing plan.

5 Determining if a New Plan is Needed

Take our quiz.

Some businesses may think that they are already well covered and do not require any additional protection. A good place to start is with a simple quiz which can help determine the possible level of vulnerability:

1. My business has documented IT security policies and procedures.
   ☐ Yes ☐ No
2. My business trains employees on our IT security policy and procedures.
   ☐ Yes ☐ No
3. My business has a documented backup and recovery plan.
   ☐ Yes ☐ No
4. My business has off-site storage of critical data backups.
   ☐ Yes ☐ No
5. If the physical structure of my business is no longer available due to a catastrophic disaster (fire, flood, etc.) I am confident I can have my business up and running again in a short period of time.
   ☐ Yes ☐ No
6. Related to the previous question: My business has defined what a "short period of time" is (3 days, 4 hours, 20 minutes).
   ☐ Yes ☐ No
7. I am confident my business has up-to-date endpoint protection (antivirus, anti-malware) installed on every desktop and laptop.
   ☐ Yes ☐ No
8. My business has an automated patch management system to keep servers and workstations up to date.
   ☐ Yes ☐ No
9. I am confident the email system for my business is well protected against spam, phishing and other email security issues.
   ☐ Yes ☐ No
10. The IT team for my business has the resources and knowledge to handle a comprehensive technology business plan internally.
    ☐ Yes ☐ No

Scoring:

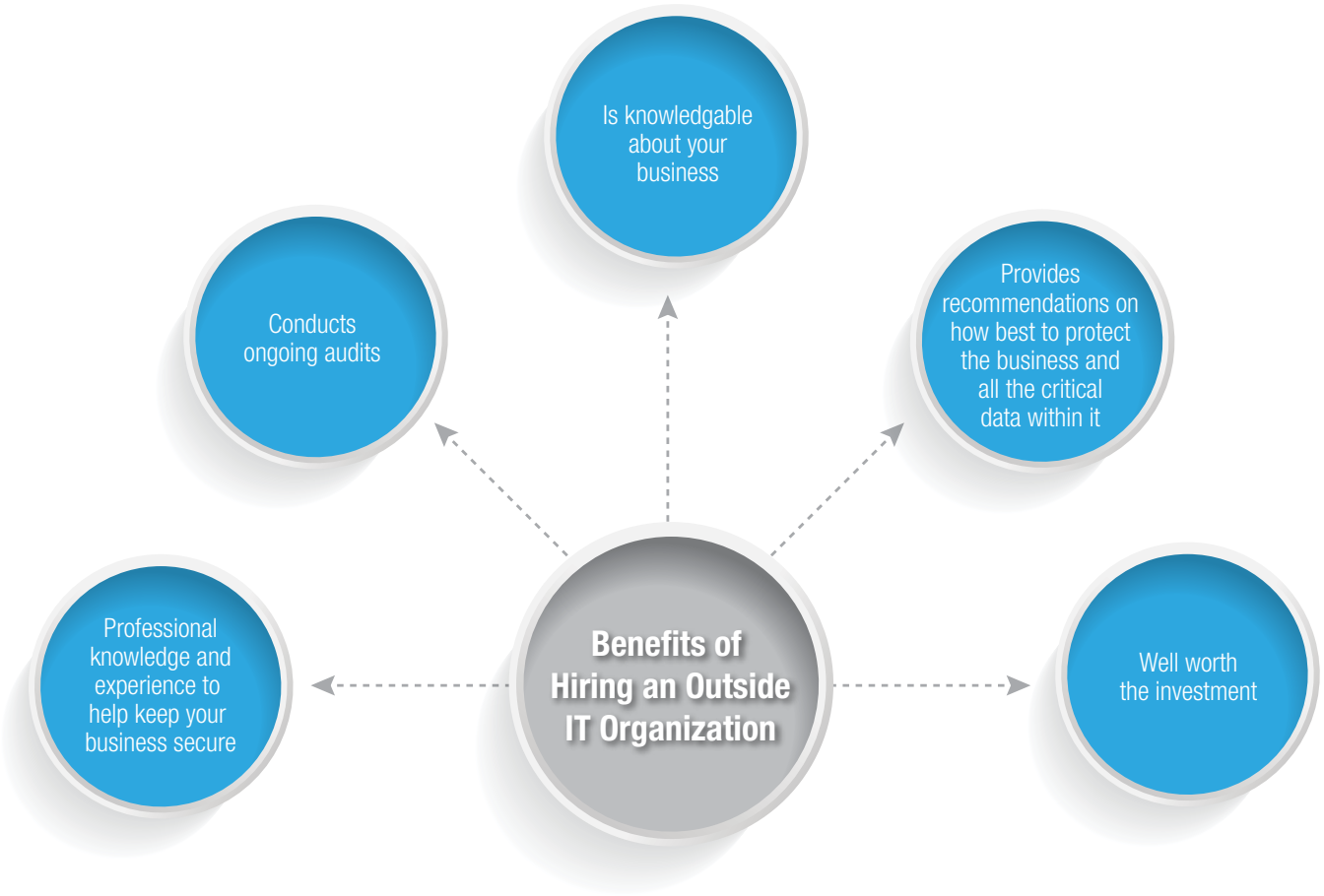
GOOD SHAPE: If you answered "Yes" to 9 or 10 of these questions, your overall business security appears to be in good shape. An assessment is still recommended to make sure you have covered all the bases.

REQUIRES FURTHER EVALUATION: If you answered "Yes" to 7 or 8 of these questions, your overall business security may be insufficient and needs further evaluation. An assessment is highly recommended to find areas of vulnerability.

REQUIRES IMMEDIATE ATTENTION: If you answered "Yes" to 6 or less of these questions, your overall business security is inadequate and needs immediate attention. An assessment is very highly recommended to find areas of vulnerability.

Depending on the answers to these questions, your business may be at great risk.
At minimum, it should warrant a discussion with the internal IT department for further review.

6 In Conclusion…



Team.

Keeping a business protected is a major effort. It takes a team to have everything implemented correctly and remain up to date. A comprehensive protection plan requires a multi-level approach as well as participation and compliance from every employee.

In 2013, one in 392 emails contained phishing attacks. Web-based attacks are up 23 percent. In 2013, 38 percent of mobile users had experienced mobile cybercrime. Potential attacks from hackers and malicious organizations are everywhere and all it takes is one vulnerability in the network to become the next Target or Adobe data breach.

Developing, implementing and maintaining a complete business protection plan is not easy. If a business does not have the internal resources to do all the work associated with a plan, it is best to seek out and employ an outside IT organization. They will have the knowledge and experience to help keep a business secure. They can come in, conduct an audit, learn about the business and then provide recommendations on how best to protect the business and all the critical data within it. If the IT team is not able to do all the work internally that comes with the size of this type of project, it is well worth the investment to bring in an expert.

7 All Covered Can Protect Your Business

Knowledge. **Protecting a business can be a daunting job without the right team in place.**

This type of project requires an internal team experienced in developing and implementing a comprehensive protection plan. If a team doesn't have the resources in house, it is best to bring in an outside organization. All Covered can provide the level of expertise needed to protect a business against all of today's risks.

Plan

All Covered can work with a company to develop a comprehensive Technology Business Plan (TBP). They will review the current business environment by holding meetings with key personnel in order to understand their strategy. They will document a business's requirements and objectives, as well as make sure all technology is properly inventoried.

All Covered has a variety of tools at hand to review a company's current security posture and identify potential problems such as user account issues, unprotected devices and configuration conflicts. Based on the data collection, they will be able to prepare a Technology Business Plan customized for that specific organization.

Secure

Once the plan has been approved by the business, All Covered will get to work with the implementation phase of the project.

One of the most important parts of a protection plan is messaging protection. Email is constantly being bombarded by spam, phishing scams, viruses and worms. All Covered can provide inbound and outbound email protection, which will block more than 99 percent of spam. Their messaging continuity program provides a seamless solution when outages take place. It provides access to email received during an outage via a secure web browser with full email functionality so a company's employees can continue to be productive and stay in contact with customers.

Email encryption is an add-on service offered by All Covered. If a business moves confidential data via email, an encryption program is highly recommended. It is especially important if a business is required to be compliant with industry or government regulations, such as HIPPA, GLBA, PCI DSS or EU PPD.

The endpoint protection provided by All Covered will shield a business against virus and malware attacks. Their antivirus program provides automated deployment of protection solutions on both servers and workstations. All Covered's anti-malware solution provides an additional layer of defense on workstations.

It can quickly detect, destroy and prevent malware through its automated deployment and continuous scanning and malware cleaning.

All Covered can provide DNS filtering to provide another layer of protection. It can block known and unknown threats by malicious domains, URLs or IPs. Unlike pure proxies, it contains botnet callbacks from infected devices over any physical servers, virtual servers, PCs and laptops.

Web content filtering is another service provided by All Covered. Their solution allows greater management control over unauthorized, unproductive workplace Internet usage. It manages the Internet experience of employees by using features such as category-based filtering, whitelists and blacklists and user-based access to specific blocked categories.

All Covered can implement automated patching so servers, workstations and remote computers are kept up to date with the latest security patches, software updates and service packs. It can scan networks for installed and missing security patches and monitor and maintain patch compliance for the entire enterprise. Another critical piece of the security plan involves periodic vulnerability testing. All Covered provides an automated monthly vulnerability scanning solution to make sure your external and internal network devices do not have any critical exposures. Since new threats are discovered almost daily, performing these scans on a monthly basis helps ensure that your network is not affected.

Protect

Once an organization's plan is developed and implemented, it requires ongoing maintenance and review. All Covered has the ability to continually protect businesses. They offer managed backup and recovery solutions for physical servers, virtual servers, PCs and laptops so data is completely protected. All Covered can also provide email archival security. Its solution provides total protection for email-based data assets and full support for industry and regulatory compliance. Although some solutions do require an occasional purchase of hardware, there is no software installation required or complicated management involved. All Covered's cloud solutions are second-to-none. The All Covered Cloud Servers focus on reducing an organization's need to continuously invest in IT-related hardware and software while increasing server uptime. The enterprise-grade cloud solution is fully managed and includes system and file backup, patch management, remote monitoring, event log tracking and technical support. These systems are all hosted within the United States in a secure private cloud datacenter, which is SSAE 16 SOC 2 compliant. Each cloud server has its own dedicated firewall, allocated RAM, disk space and bandwidth, so any business can have confidence that their data will be online and available every minute of every day.

8 About All Covered

All Covered is a division of Konica Minolta Business Solutions and is an industry leader when it comes to IT services. We can provide cloud hosting, virtualization and data center relocation. When a security audit is required and a protection plan needs development, All Covered has the knowledge and track record to help navigate your IT project to successful completion. Contact All Covered toll-free at 866-446-1133 or visit www.allcovered.com to gain an unprecedented level of experience and support when it comes to IT management.

ABOUT KONICA MINOLTA

Konica Minolta can help give shape to your ideas and partner with you to achieve your corporate objectives. Contact us to realize opportunities in:

Information Management
- Enterprise Content Management (ECM)
- Document Management
- Automated Workflow Solutions
- Business Process Automation
- Security and Compliance
- Mobility

IT Services
- Application Services
- IT Security Assessments
- Hybrid and Private Cloud
- Business Continuity
- 24/7 Help Desk
- IT Resources and Consulting

Technology
- Office Multifunction Business Solutions
- Commercial and Production Printers
- 3D Printers
- Wide Format Printers
- Laptops, Desktops and Computer Hardware
- Servers and Networking Equipment
- Optimized Print Services (OPS)
- Facilities Management

KONICA MINOLTA

KONICA MINOLTA BUSINESS SOLUTIONS U.S.A., INC.
100 Williams Drive, Ramsey, New Jersey 07446

CountOnKonicaMinolta.com

Item #: XXXXXXXXX
1/15-I