MRE Technology SERVICES

WHITE PAPER

# SECURING DATA:
# WHAT AN EXECUTIVE NEEDS TO KNOW

AN EXECUTIVE BRIEF FROM STEPHEN WEBSTER, MRE'S CHIEF TECHNOLOGY OFFICER

## Even a casual observer of the morning news is aware of the dangers hackers pose to American businesses.

As an executive, you may be called upon to make decisions about how to protect your company's data even if technology issues don't normally fall under your responsibilities or expertise. Don't worry — you don't have to be a technology expert to make informed decisions about data protection.

> While every company has different security needs, a few simple guidelines can help give you a framework for making good decisions.

## KNOW YOUR DATA

The first step in protecting your data is to know what data you have that might be valuable to cyber-thieves. Do you have volumes of private customer data? Do you have proprietary information that competitors could use to gain an advantage? Are you storing confidential data critical to your business strategy? The more valuable the data, the more security it will need.

For firms with relatively small amounts of data, a good firewall and password policy should protect the company. Keep firewall software up-to-date. Use passwords with numbers, letters and special characters, and change them regularly. In addition, it is imperative to have working back-ups of the company's key data and systems in place. With the rise of Ransomware and Malware aimed at these components, a backup is critical for protection and recovery in the case of an attack.

Companies with large amounts of proprietary data, intellectual property, or other mission-critical information will need to consider stronger measures to safeguard their data. The more valuable the data, the more capable the intruder coming after it is likely to be.

Also, be aware of what data you are legally required to protect. Privacy laws can allow corporate officials to be held personally liable if they don't take adequate measures to secure certain sensitive information about customers and employees. If you don't know what you are required to protect, ask an information security or legal expert for help.

Remember, ignorance is no defense from the law. Expert advice can help you avoid legal troubles while you handle the setbacks that result from your data being compromised by hackers.

## SET THE RIGHT BUDGET

How much money you need to spend to protect your data is a function of the value of that data. Spending too little on security can leave you and your firm open to some nasty surprises as motivated thieves circumvent your countermeasures. At the same time, it is possible to overprotect data out of fear and waste resources that could be better spent elsewhere. You have to decide on the proper balance to meet the needs of your firm.

As a rule of thumb, firms should spend 5 to 12 percent of revenue on IT infrastructure. About 10 to 20 percent of that should be dedicated to IT security infrastructure. For many firms, this amounts to a sizeable expenditure. In such cases, it is a good idea to talk to outside IT security specialists to help establish what security level you need and what options are available. IT security is a specialty skill that is outside the expertise of many good IT departments. Security specialists can advise you on what you need to protect you from the most likely threats faced by your sensitive data. They can also recommend options that return greater security at a greater value.

## PUT THE RIGHT PROCESSES IN PLACE

The human element is the single greatest risk in IT security. Good security is often foiled by bad behavior of employees. Workers use weak passwords, lose laptops, open suspicious e-mail attachments, and sometimes let strangers access systems without thinking of the consequences. Employees can also forget to log out of computers and leave passwords lying out in the open. Furthermore, employees often download unapproved software, which can be a pathway for attackers. Most security breaches ultimately lead back to negligent behaviors. The best solution for this giant security hole is to have good procedures with proper controls and regular training in their use. Don't count on technology to protect you from bad habits.

## THINK LAYERS

No security system is foolproof. The key is to put enough layers of defense in place to discourage hackers and cause them to look for easier prey. Too many companies make the mistake of building a strong outer shell that they think is impenetrable. Once an intruder breaches that shell, the entire corporate data infrastructure is open. Instead, you want layers within layers of security. This greatly increases the chances of a hacker becoming frustrated or detected before he or she can reach sensitive information. A good system should also leave an extensive audit trail. If nothing else, this gives the security experts a clear path to follow in the event of a breach to track down and patch the hole in the defenses.

## STAY CURRENT

You can never let your guard down. Cutting-edge viruses are constantly being developed to enable new methods of bypassing a system's security. It is vital to stay up to date on current cyber security trends and technology to prevent and prepare for security breaches.

In their effort to stay current, software companies are constantly releasing new patches for their applications. Delaying an update allows cybercriminals more time to become familiar with the targeted system and puts your system at greater risk. For example, the recent WannaCry and Petya ransomware attacks could have been prevented through proper and timely patching of the Microsoft operating system.

## RECOVERY

So what do you do if all of your security fails, and you wake up one morning to find your company has been breached and its data stolen? The first rule is to stay calm. Figure out exactly what has happened and make sure you understand all the facts. The worst thing you can do is overreact.

Don't shut down your entire network in a panic and stay offline until you feel safe. Determine what was taken and who will be affected by the stolen data. Then alert those people as soon as possible. Trying to hide a data breach that puts other people in jeopardy can damage your corporate image and reputation, which in the end may do more injury to the firm than the data breach.

Alerting the right people includes alerting the authorities, such as the FBI. Every country has an organization that should be contacted as soon as you assess what has happened. They can help deal with the problem and possibly help track down the threat.

In cases of a virus requesting a payment, it is recommended to never pay the ransom. Don't try to solve the problem on your own or waste time thinking about striking back or taking revenge. Many hacking attacks are undertaken by criminal organizations and even foreign governments who likely have more resources than you. The best advice is to focus on patching the holes and taking care of your customers. Let the proper authorities find the perpetrator and take appropriate legal action.

A security breach will often require outside experts to help resolve all the problems. Not only do IT security professionals have the specialized knowledge needed to help, they can provide good advice that isn't tainted by the emotional shock of the breach that is affecting inside personnel. Don't be afraid to admit when you need help.

## PUBLIC RELATIONS

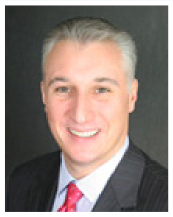
If members of the public were affected by the breach, the right thing to do is let them know with a public announcement. Be clear about who is at risk and reassure them that you are taking measures to fix it.

Put measures in place to help them recover. If personal credit information was taken, offer to pay for a year of credit monitoring or some other compensation. Not only is this the responsible thing to do, it can also further protect your brand from credibility damage.

At this point in the crisis, a good public relations department can be invaluable in crafting a message and creating a proper response plan. If your company doesn't have a public relations department, consider hiring a reputable outside firm to assist you.

## CONCLUSION

You don't have to be a technology expert to make good management decisions in regards to guarding data as long as you remember a few simple guidelines. Make sure you understand what your valuable data is and to whom it has value. Invest properly in data security and consult experts when needed. Support the technology you purchase with good policies that are monitored for compliance and constantly reinforced through training.  Be proactive in ensuring that your defenses are properly layered and employees informed. In the event you do get hacked, respond appropriately and transparently with help from the proper authorities. The biggest thing to remember is to make it as hard as possible for unauthorized users to access your valuable data. Hackers seek out the path of least resistance. You don't have to make your network an impregnable fortress. You have to make it just hard enough to discourage intruders so they seek easier targets elsewhere.



## ABOUT THE AUTHOR

***Stephen Webster, Chief Technology Officer, MRE Consulting, Ltd.***

*Stephen is a recognized expert at designing and implementing infrastructure solutions and services for Global Fortune 250 companies. He has provided expert commentary on topics ranging from data security to cloud computing, and has been featured on Bauer Business Focus, NPR and CBS Radio.*