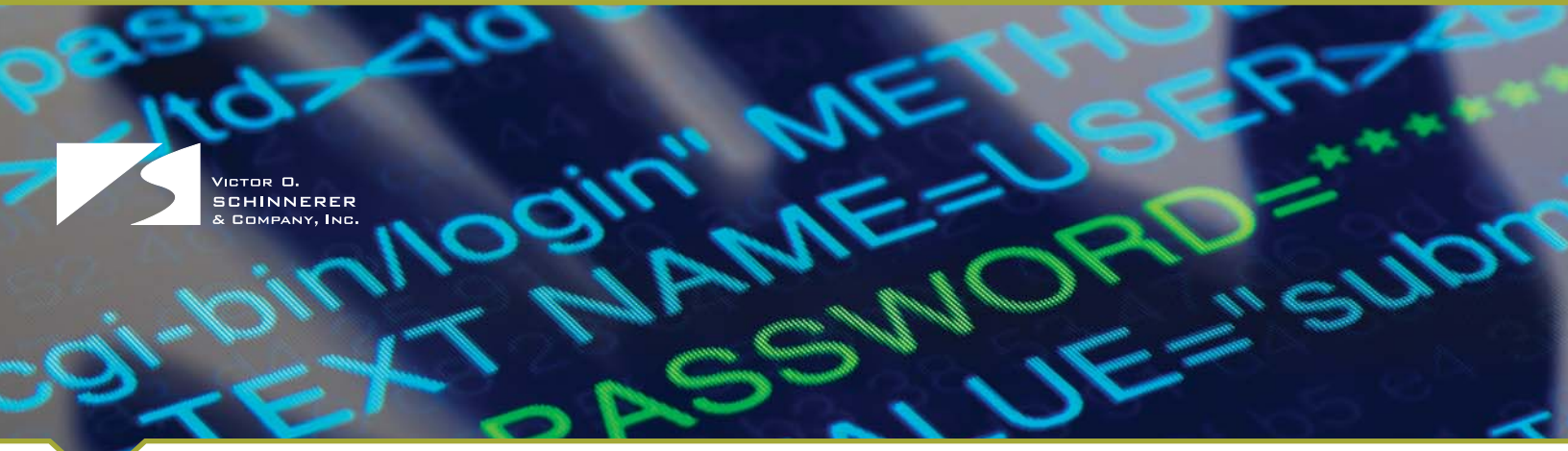

PROTECT FIRM OPERATIONS FROM THE DISASTER OF RANSOMWARE

MANAGEMENT ADVISORY

In this age of increasing cyber crime, professional service firms should anticipate that their business files and systems could be held for extortion payments. Unfortunately, some have already been victims of ransomware demands. Firms that have experienced the chaos and despair that a ransomware attack causes know that it is a largely self-inflicted injury that is costly, debilitating, and damaging to a firm's reputation. Firms that have yet to be attacked should know that they can protect their operations through staff education, comprehensive data protection procedures, and insurance coverage that is ready to help if an attack occurs.

UNDERSTAND WHAT RANSOMWARE DOES

Ransomware is malicious software that digitally locks a victim's computer systems or files until they pay a ransom to have the systems or files unlocked. Once the malware gets a hold of an infected computer, it will encrypt files and folders on local drives as well as any attached drives, backup drives, and possibly other computers on the same network. After the initial attack, users will be unable to access their data and will receive extortion demands. A ransom message is displayed demanding payment to unlock encrypted files.

While law enforcement advice has been to decline to pay extortion demands—there is no incentive for criminals to actually provide the key to unlock files and payments only encourage further criminal activity—many firms find that their earlier deficiencies in defending their operations from such attacks force them to gamble on recovering files by paying the ransom. It appears that the typical victims pay criminals between $200 and $10,000 to regain access to their systems or files.

A ransomware attack can be terrifying—encrypted files or systems may essentially be considered damaged beyond repair. And with that damage a firm could be exposed to tremendous internal costs, lost productivity, breach of contract claims, and even allegations of negligence in the firm's performance of professional services. With proper preparation, such an incident can result in nothing more than a nuisance.

PROVIDE EMPLOYEES WITH NECESSARY EDUCATION

One of the most effective ways that businesses can protect their systems against ransomware is to put employees through an effective security-awareness training program. Only in recent years has the importance of this layer of security been recognized. Often, firms have relied upon software as a prophylactic for these types of situations, but software by itself is not enough. Users must be trained to prevent such attacks from happening in the first place.

Much of the effective prevention is based on appropriate internet usage. The same precautions should be used on a mobile device as on a computer when using the internet. Employees should understand that pop-up blockers assist in preventing the spread of malicious software. To avoid accidental clicks on or within pop-ups it's best to prevent them from

appearing in the first place. And malware can come in downloadable games, file-sharing programs, and customized toolbars.

Employees should constantly be reminded not to open attachments in unsolicited emails even if they appear to come from someone in the firm or on the employee's contact list. Clicking on a link contained in an unsolicited email, even if it looks safe, is far more dangerous than closing the email and going to an organization's website directly.

A simple knowledge of what red flags to be aware of can make a huge difference in the ability of a user to discern malicious links and malware from legitimate emails. As the methods hackers and malware creators use to trick users are constantly changing, it is important to keep users up-to-date on not only the basics of internet and email security, but also the ever-changing ransomware attack types and other threats.

FOLLOW DETERRENT AND BACK-UP PROCEDURES

The most effective deterrent against the damage that ransomware can cause is having a regularly updated system backup. If a firm can return its system to a restoration point or clean up its system and restore lost documents from backup, it can prevent much of the costly disruptions caused by an attack. A regular backup regimen to an external drive or backup service—one that is not assigned a drive letter or is disconnected when it is not performing backup—is essential. It is crucial to have a backup system either in a cloud network or some location outside the firm's network where hackers cannot reach because backups that are easily accessible to a ransomware-infected computer might be encrypted along with the files that they are intended to backstop.

Backing up content is not a static process; every backup should be verified. Firms should perform backups in real time and then test those backups. That way if a firm is targeted the firm can have its system wiped clean and files reloaded instead of paying a ransom to get data back.

There are a number of other things firms can do to help prevent malware infections. For example:

- Use up-to-date security software;
- Turn on the network's firewall;
- Limit user privileges;
- Use trusted locations for files in the firm's enterprise; and
- Enable automated patches for the operating system and web browser.

Many firms have found ways to break their network into smaller parts as opposed to having everyone in a large organization using a single server to access files. That way, even if a server gets infected it will not spread ransomware to all firm systems and computers.

Time is critical for a firm faced with a ransomware deadline. Online extortionists typically give firms a very specific time limit within which to pay; after the deadline passes they sharply increase the ransom demand. Attackers have become increasingly better at knowing what a firm can afford, knowing exactly when to strike, and limiting the ability of firms to figure out if they can unlock or sufficiently restore the data without paying any ransom. This is especially true with ransomware attacks that come from former—or perhaps current—employees (not all attacks are international in scope). With the easy availability of ransomware, some attacks are launched by those familiar with a firm's operations.

It is important to have a plan in place that describes what needs to happen in the event of a ransomware attack. An inventory of critical data assets, knowledge of where it is stored and duplicated, and an evaluation of the impact of any loss or unavailability that data will cause is part of the plan.

RECOGNIZE INSURANCE AS AN ESSENTIAL FORM OF PROTECTION

Another essential element of a response plan for ransomware attacks is appropriate insurance coverage.

Too often, firms think that professional liability insurance covers all of their exposures. That is not the case. Professional liability coverage only applies if the underlying cause of action was based on a wrongful act or omission in the performance of professional services, and not on a wrongful act or omission in the operation of a business that happens to provide professional services. That is why Schinnerer developed a comprehensive cyber policy and program. Schinnerer's Cyber Protection Package provides broad coverage for professional service firms that can include the following:

- **Breach Rectification, Including Digital Property Replacement Coverage:** The policy includes coverage for business interruption and digital asset losses, including tools to get a firm back to productive service as quickly as possible and to protect the firm's reputation. Coverage includes digital property replacement that pays the reasonable and necessary cost to replace, restore, or reconstitute digital property from written or electronic records. This is essential coverage to mitigate the harm of cyber extortion.
- **Cyber Breach Response Team:** Coverage includes access to expert risk management tools that decrease a firm's exposure by providing industry-specific guidance. If a ransomware attack occurs, an expert team provides legal services and technical support to assist policyholders. The team works closely with the firm and, when necessary, with forensic and crisis management consultants to identify the cause of the breach, determine its scope, and formulate the appropriate response. In the event of a breach, a privacy attorney will be assigned to the case and promptly respond to and investigate any suspected or actual event.

PREPARE FOR THE BUSINESS RISKS OF RANSOMWARE

Not all ransomware is identical. The forms are constantly changing and becoming more sophisticated, and they are becoming easier for cyber criminals to use. The trend has significantly heightened the need for firms to have measures in place for blocking threats and mitigating damage as much as possible.

The key thing that makes a piece of malware "ransomware" is that it attempts to extort a direct payment from a firm. The key thing that makes ransomware a manageable risk is preparation and proper insurance coverage.

ADDITIONAL RESOURCES

The federal government and many associations and private entities provide additional information on cyber risks. Firms can go to the FBI's cyber division at **www.fbi.gov** and report incidents through the Internet Crime Complaint Center at **www.ic3.gov**. For more information on how Schinnerer's Cyber Protection Package can help protect a firm from many cyber liability exposures, go to **www.Schinnerer.com/cyber_liability_insurance.aspx**.

Visit **www.Schinnerer.com/AEriskmanagement** for more information or contact us at **vos.RMeducation@Schinnerer.com**.

For more information on practice management, please visit our website at **www.Schinnerer.com/AEriskmanagement**, or you can reach our Risk Management Department at 301-961-9878, fax at 301-951-5496, or email at **vos.RMeducation@Schinnerer.com**.

Victor O. Schinnerer & Company, Inc.
Two Wisconsin Circle
Chevy Chase, Maryland 20815