RIVER RUN

5 major network threats you cannot afford to ignore

How River Run will help you secure your network

The threat is real.

- 71% of security breaches target small businesses *(IDC)*
- 27% of small businesses have no cybersecurity protocols *(Time Warner Business)*
- A data security breach can harm a small company's reputation by 17-31%. *(Ponemon Institute)*
- 60% of small businesses that suffer a cyberattack go out of business within 6 months due to loss of sales or cost of recovery. *(Symantec)*

A breach of your network security can be very costly in terms of lost data, customer records, employee productivity, reputation and revenue. Do not leave it to chance thinking that it cannot happen to you. There's too much at stake.

Today, small to medium-size companies are facing greater network security threats than ever. From ransomware to socially engineered browser hacks, a business that is not properly protected can be brought to its knees - without warning.

Many owners of small to medium-sized businesses do not think they are at risk. They do not think it could happen to them. But they are wrong, explains Matthew Minikel, Security Officer at River Run Computers, Inc. "Small businesses are even more at risk than larger ones, because they don't have the resources to defend themselves. In addition, they may not be as vigilant at server updates and other preventative measures as their larger counterparts."

This eGuide contains five network security threats to small to medium-sized companies, and how you can protect your firm against them:

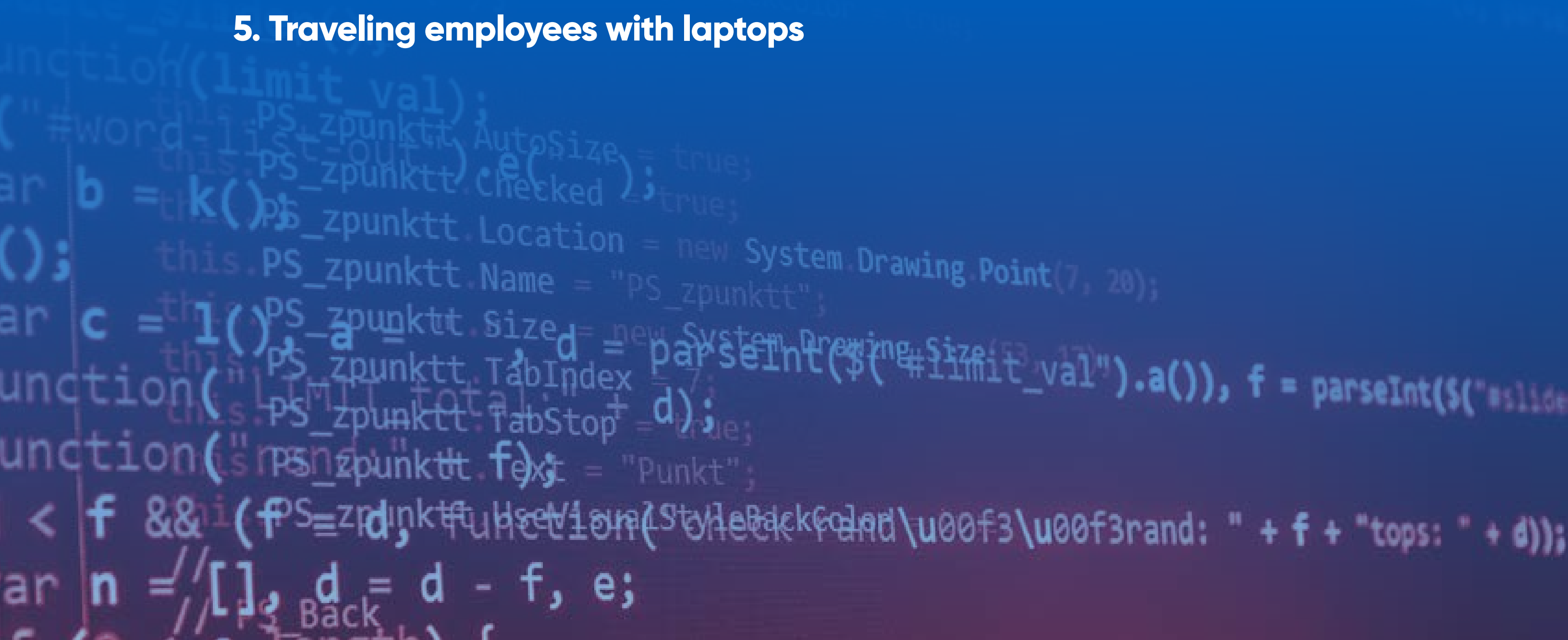
1. Ransomware

2. Inadequate password security

3. Employees stealing data

4. Enabling employees to access the network with mobile devices

5. Traveling employees with laptops



Threat #1 : Ransomware

Ransomware is a type of malware that encrypts certain file types on infected servers and computers. It forces companies to pay ransom to the hacker who created it to get a decrypt key. It can enter your network in two different ways:

1. **Via email:** One of your employees clicks on a link to a malicious website, which downloads a small, unobtrusive piece of malware through their browser. It then looks for shared drives that the person's account has read/write access to, and uses that beachhead to eventually obtain network administrator rights. At each step it encrypts any hard drives it encounters, making them unusable.

2. **Via the network:** This type of bot enters your network by exploiting an open or inadequately protected port on your server.

Minikel recalls one California hospital whose data was held for ransom for $17,000. Until it paid this amount, all of its patient records were inaccessible. Unless you have a real-time backup of all of the drives on your network, you may have no choice but to pay the ransom to regain access to your files.

The best defenses against ransomware are to educate your employees on how to identify suspicious links and to have a reliable backup process.

The former can be done with pro-active testing and training. The latter ensures that if any network or local drives are compromised, they can be quickly wiped and restored using up-to-date backup copies.

Minikel recommends a two-tiered strategy: a backup storage device on site which also communicates with secure enterprise cloud storage. This approach ensures that your company's data is always stored at least three places, one of which is off-site.

! **New ransomware families have grown 600% since December 2015.** *(Barkley Blog)*

Threat #2 : Inadequate password security

Inadequate network passwords are another potential threat to companies of all sizes. Often, computer users on a network will recycle the same two to three passwords over and over. Some use the same password for an extended period of time – because they aren't required to change them.

Minikel recommends that small and medium-size companies change employee passwords at least twice a year. If they are required to comply with data privacy standards, then employee passwords should be updated every 90 days.

Companies should also have strict policies that prohibit password reuse and require a certain level of complexity for acceptable passwords. Two-factor passwords provide another level of protection on top of conventional network passwords. Companies like Duo and Google offer two-factor authentication services that work with mobile devices. When an employee logs into the network, it communicates with these third-party authenticators to ensure that the login is coming from a legitimate location. Biometric authentication, which uses a small device to scan the user's thumbprint or retina, is an enhanced form of two factor security.

Frequently, employees use the same password for their online services at home as they do for the work network. Why is this a problem? When large consumer sites are hacked and millions of records are stolen, the data they get away with may include unencrypted usernames and passwords. A skilled hacker can attempt to break into a desktop or server by trying the stolen usernames and passwords.

90% of employee passwords can be cracked within 6 hours. *(LogMeIn)*
65% of people use the same password everywhere. *(LogMeIn)*

Threat #3 : Employees stealing data

Sometimes, an employee with access to the company's customer information or other sensitive data leaves the company and attempts to copy files and records and take this valuable data with them. To help prevent this, Minikel recommends three approaches:

- The firm's employee handbook and network use policy should clearly prohibit employees from taking any corporate data for their personal use.
- Change control can be set up to prevent disgruntled employees from copying, moving or destroying key files.
- Auditing should be enabled on the network – especially on those servers that host sensitive data. IT administrators and service providers should be able to monitor who is accessing these resources and when they are being assessed.

! **66% of companies see insider data theft.** *(Accenture)*

Threat #4 : Enabling employees to access the network with mobile devices

Frequently, small to medium-size companies allow employees to access the wireless Internet services on their networks. Minikel recommends that office managers and IT administrators rethink this policy. These devices can allow malware to "jump" from the mobile devices to your network, where it can cause considerable damage.

"There's no way of knowing exactly what software is running on these consumer devices," he warns. "If you must enable employees to check company email or browse the Internet from their mobile devices, be sure they have the proper security software installed." For example, if your company uses an Exchange server on your network, it can be commanded to send a signal to a lost or stolen smart phone to wipe its memory.

"As a general rule, employees should not be walking around with any corporate data on their personal mobile devices," Minikel adds.

1 in 5 organizations have suffered a mobile security breach, primarily driven by malware and malicious WiFi. *(BYOD & Mobile Security Spotlight Report)*

Threat #5 : Traveling employees with laptops

Employees traveling with laptops represent another potential threat to the security of your network. Frequently, they are accessing the Internet via unsecured wireless connections at hotels, coffee shops and other remote locations. Unsecured locations expose them to many types of infections.

If an employee must carry corporate data with them on a laptop, the hard drive should be encrypted. Ideally, no corporate data should "live" on that device. Employees should only access the corporate data and network via a Virtual Private Network (VPN), a secure connection that provides an encrypted tunnel between the remote user and the corporate network.

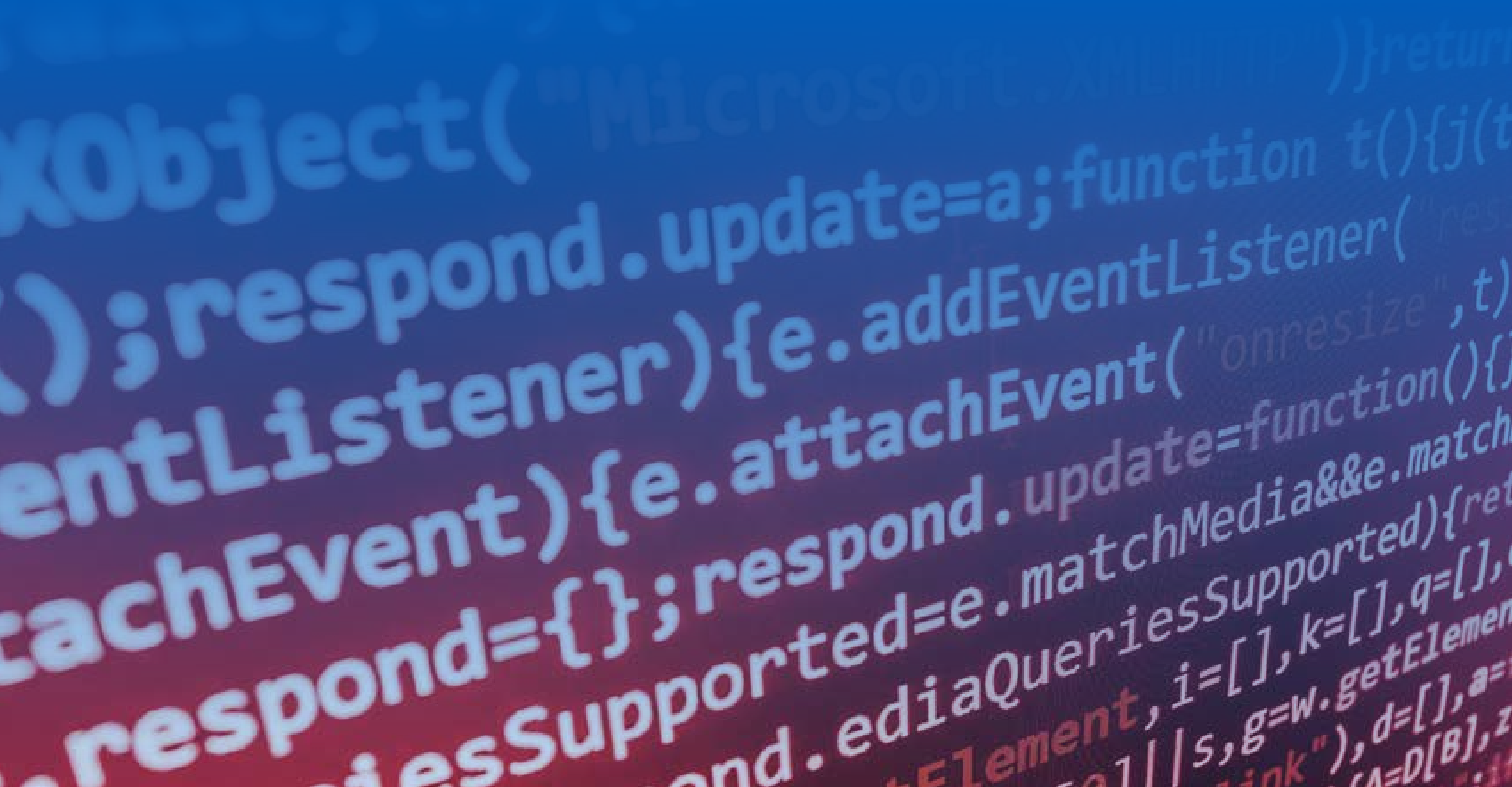
45% of employees don't worry about security of work-related data on mobile. *(Ponemon Institute)*

Do not put your business and its reputation at risk. We can help.

Cyberattacks can potentially put your company out of business, or severely cripple it. The risks are growing every day, and your company may be a hacker's next target.

Do not go it alone. River Run offers comprehensive vulnerability and penetration testing. We will identify and close any "back doors" where hackers, malware and bots can sneak in. Then, we will scan your network continuously, monitoring it for intrusions, 24/7. Finally, we will help you develop policies to help secure your company's valuable data from the inside out.

Contact us to discuss your needs at 414-228-7474.


XObject("Microsoft.XMLHTTP")}return
();respond.update=a;function t(){j(t
entListener){e.addEventListener("resize",t)
achEvent){e.attachEvent("onresize",t)
respond={};respond.update=function(){
iesSupported=e.matchMedia&&e.match
ond.ediaQueriesSupported){ret
Element,i=[],k=[],q=[],
s,g=w.getElemen
ink"),d=[],a=

RIVER RUN

414-228-7474 phone
414-228-5009 support
414-228-3076 after hours emergency
river-run.com

2320 W. Camden Road | Glendale, WI 53209