Cybersecurity in the Wake of the Conflict in Ukraine:

How to Keep Your Company Safe from Russian Hacks

by Susan Gosselin

Russia has now moved troops into Ukraine, and the fierce ground warfare this has generated has riveted the attention of the world. But did you know that one of the most important battlefields is in cyberspace – and this could have very real implications for your business?

An Unprecedented Cyber War: Why American Businesses Should Be Concerned – and Prepared

For perhaps one of the first times in history, official, open cyber warfare has been declared, with Ukraine calling on a volunteer cyber army to disrupt the Russian government and Russian assets, and the global hacktivist group Anonymous vowing its help, as well. Russia, for its part, already has one of the world's most advanced cyber armies. It's no secret that Russian hackers, whether they're sanctioned by the government or not, have been attacking American government and business targets for years.

In fact, 2021 saw the largest leap in cyberattacks in history. According to the 2022 Cyber Threat report released by SonicWall, ransomware attacks rose by 104 percent in North America last year. And that's bad enough. But government sites saw a 1,885 percent increase in attacks, and healthcare industry sites faced a 755 percent increase.

And all this was before the invasion of Ukraine.

"Russia has always had a strong cyberattack presence through state-supported and state-protected threat actors. So, they have a tremendous natural resource at their disposal now," said Nick McCourt, vCISO and Security Engineer at Integris. "With the value of the ruble dropping, and the pressure mounting on them from sanctions and cyberattacks, it's possible Russia may be looking at ransoming US targets to disrupt business and generate much-needed income. Whether those threats become real or not, every business should be taking steps to be prepared," he added.

Shields Up: The US Government Calls on American Companies to Reinforce their Cyber Defenses

For its part, the US Government has been quick to note that the Russian government hasn't made specific threats against American businesses – yet. But they are urgently warning American businesses to shore up their cyber defenses to prepare for the worst. They've created the Shields Up program to help.

The program offers specific guidelines for companies to follow, so they can more readily find the holes in their cybersecurity program. They're offering free threat scans, as well.

Most tellingly, they are asking companies to lower the threshold for reporting cyberattacks to the

government. They are looking for businesses to report any coordinated cyberattacks to the FBI – an effort that will help the government track the nature and severity of incidents across the nation.

Your Cybersecurity Defenses: What Every Company Should Be Doing Now

Fortunately, cybersecurity tools are more powerful and plentiful than ever. In the past few years, products that were only available to enterprise-grade organizations are now being scaled for even the smallest of companies. That means most of these tools are priced by the size of your data needs or the number of users on your network. If you've been putting off cybersecurity upgrades because of fears your company can't afford them, now is definitely the time to get off the fence. You might be surprised to find that high-end cybersecurity tools are more doable than you think.

Shields Up is a call to action from our government to safeguard the digital infrastructure that runs American business. Every company needs to do its part. If you don't currently have these protections, we strongly recommend you put them in place, as quickly as you can.

Offsite backups

Backing up a copy of your data to your onsite server is a dangerous game. Not only does this put you at risk of natural disasters, but it opens the door to hackers to hold your running and backup data hostage. Every company should be backing up their data, every few minutes to an offsite, cloud-based server. For your company's safety, those backups should be "immutable," or, to put it more plainly, unable to be erased. In the event you do get hacked, you can redownload your systems and be ready to go within minutes. No ransom? No problem.

An Incident Response Management Plan

What would happen if a data breach occurred at your company? Do you have experts who can help you mitigate the damage? Are resources in place, and roles defined on your technical team? Who notifies customers that their data has been compromised? All this should be put in writing, and updated regularly, so there's no time lost when the worst happens.

Perhaps even more important, do you have the tools to do forensic analysis and figure out what went wrong, where? If you've invested in Security Information and Event Management (SIEM) and Managed Detection Response (MDR) tools, you'll have visibility across your network to see where threat actors have been lurking in your system. Crucially, you'll have the ability to manage your logs, and create breach reports. If you have a cyber liability insurance policy, this information is needed to make a claim.

Cyber Liability Insurance

While a good cyber liability insurance policy won't prevent a cyberattack, it can ensure your company isn't taken down by one. After all, the average ransomware payment has crept up 82 percent in 2021, to $570,000, according to a recent report by Palo Alto Network's Unit 42. And that's to say nothing of the thousands you'll spend on recovery costs, and the thousands you'll lose in lost business and reputation.

A good cyber liability policy costs most small businesses between $1,000 and $3,000 – a small price to pay for peace of mind. However, it's important to remember that insurers have high standards for the companies they cover, and you'll be expected to have a full battery of cyber security defenses to qualify. For more information on what insurers look for and how these policies work, check out our recent webinar on getting and staying insured against cyber risk.

Virtual Private Networks and Multi-factor Authentication

Employees now need the ability to work either in or out of the office. And most businesses have shifted to this kind of flexible arrangement. But if you're relying on just a simple office firewall or anti-virus software, you're putting your company at risk every time an employee signs in through public Wi-Fi. Every company

should have a virtual private network – a secured channel that encrypts data in transit. Employees also should have multi-factor authentication systems for their logins, requiring secondary sign-ins through a mobile app like Duo, or fingerprint scans, or other more advanced identification programs.

If you're considering moving your workforce to cloud-based systems, now might be the time. Products like Microsoft's Windows 365 CloudPC can put your entire operating system on an encrypted cloud and allow your employees to work safely from any device, anywhere. Other cloud services such as AWS and VMWare Horizon View can offer many of the same benefits.

Employee Cybersecurity Training

Did you know that 74 percent of organizations say they've been breached because of employees breaking security rules? This latest report from Arlington Research isn't terribly surprising to those of us in the IT space. That's why we recommend that companies spend time and resources shoring up their most important defense: their employees. Employees who know how to spot email phishing, impersonations or social engineering attacks can stop the vast majority of hacks before they even start. Fortunately, there are a wealth of very good cybersecurity training programs that can be administered to your staff online, with testing to prove that they've mastered the concepts.

Your managed service IT provider should also be able to set your company up with incursion testing, to decide where the weaknesses are in your network. With analysis and training, you'll truly have an educated, empowered, and cyber safe staff.

There's Never Been a Better Time to Secure Your Cyber Defenses

Most companies looking to upgrade their systems can do so in a matter of weeks, or even days, McCourt said. Typically, the cyber security tools you lack can be layered onto your existing protections.

"It's hard not to be rattled by these headlines. There's been an explosion of cyber threats over the last year," McCourt said. "But the good news is, there is a tool to help counter every threat. They're readily available, and manageable for every company with help from a Managed Services Provider or MSSP."

Are you ready to scan for your organization's vulnerabilities? Integris can help. Contact us and set up a consultation, today.