How to Secure Your System & Remote Connectivity Against Cyber-Attacks

MAR 15, 2022 • CATEGORY: TECHNOLOGY INSIGHTS • BY MARY ANNE BALLOUZ

• 12 MIN READ

The last time I was in London was just after Christmas 2019. I had been to this incredible, vibrant city before but had never seen the changing of the guard at Buckingham Palace, so my friend and I went to watch one morning. As you can imagine, many people were there, as were lots of police, both on the ground and on horseback. Every five minutes, police officers would shout to the crowd to be careful about pickpockets, to watch personal items. Even in daylight, with police around, pickpockets were there. Of course, whenever you travel, you know to be careful about your personal items like your backpack, purse, and wallet. You generally (and hopefully) have a heightened awareness about the potential of pickpockets, especially in touristy places. I mean that is the reality of big cities: gullible, careless tourists attract these criminals. And yet, there are still people who do not take the necessary precautions, who let their guards down, and who then end up as victims of such crimes.

And so it is with cyber-attacks. Cyber threats are unfortunately prevalent throughout our technologically advanced world with technologically advanced IT systems. More and

more you hear about companies that have been compromised, either by some malware or more recently ransomware. Malware or "**mal**icious soft**ware**" is any software program that infiltrates an IT system, copying itself and infecting the system resulting in disruption and damage. Ransomware is a type of malware designed to gain control of the system, blocking access until a ransom is paid. Companies that have been victims of these cybercrimes most probably did not take the appropriate security measures to ensure proper defense against these attacks. And so, the question begs: "What could these companies have done differently?" "What precautions could they have taken?" These questions are particularly important when an organization's operations include the need for remote connectivity as this is a potential point of weakness that hackers like to target. Let's find out how to secure your system and remote connectivity against cyber-attacks by first looking at some cybersecurity stats and examples of how other companies were breached.

Some Cyber-Attack Stats & Examples

Last year, 2021, marked an incredible increase in cybercrime with high profile attacks such as Colonial Pipeline and Solar Winds among others that resulted in significant security-related and economic impacts. Hackers went after all businesses, no matter the size; small and medium businesses were not immune. Security weaknesses in supply chains and critical infrastructures were also targeted at the highest rate ever. And this trend has continued into 2022. Statistics from a study of penetration testing ("pentesting") projects from **Positive Technologies**, which was conducted amongst a number of industry verticals, showed that in 93% of the cyber-attack cases, external attackers found a way into breaching an organization's network and gained access to local resources as pivot points to perform more widespread damage. Additionally, in advanced persistent threats, more than 90% of attackers were able to find a way into the targeted network. And year by year, attack frequency has increased by more than 50% on a weekly basis for the industry verticals that we're interested in, such as manufacturing, oil and gas, water, wastewater, chemicals, and other broader OT sectors. (Check out the webcast "**Hardening Your System Against Cyber Attacks**" for more stats on increasing cybercrime.)

So, let's talk about a couple of the different attacks that happened in 2021. For SolarWinds, bad actors attacked the company by slipping malicious code into an update to Orion software. The cost is undetermined, but it is estimated that around 18,000 customers downloaded that malicious software. This method used routine software

updates like the ones you click and don't even think about. The second cyber-attack I want to bring up, which was a ransomware attack, is Brenntag. In fact, this attack is one of the most expensive ransomware attacks to date; it cost the company $4.4 million. The attack group Darkside, which was also responsible for the Colonial Pipeline attack, purchased RDP credentials on the dark web and used that publicly accessible RDP node as a pivot point into the network. Once the attackers were in, they ransomed over 150 gigabytes of data from the North American Division of Brenntag. So how to defend against cyber threats? The first step is replacing ineffective outdated "security" measures that just don't work.

Ineffective Outdated "Security" Measures that Need to be Replaced

Too many companies are still using ineffective outdated "security" measures. The first and second measures include static VPNs and those built-for-IT remote access tools that don't take into consideration what an OT network looks like or what it needs to successfully operate in high-stress critical environments. These are environments where you need people to get to problems on the order of seconds, not minutes or hours, and for sure not days. Third, every vendor has their own security methods. Some, like ICONICS, care deeply about your security, and they're making sure that their proxies put your network security first (watch our webcast "**Hardening Your System Against Cyber Attacks**" for more details). Unfortunately, there are plenty of other vendors that do not take such precautions so be wary. Red flags include dropping a backdoor into your network, so they can get to their devices quickly. But when that backdoor is publicly accessible, it opens a huge door to your otherwise flat network. So seemingly innocuous remote updates can introduce widespread malware into your networks and create pivot points for downstream breaches.

The fourth measure to watch out for is "Shadow IT" or unsecure remote access tools. These are the ones that punch holes through your firewalls, your meticulously crafted firewalls. By punching a hole through that firewall, you're not only providing access to your network to the right person, but you're also providing it to the wrong people at the same time. And to summarize the fifth and sixth, there are those who say, "I'm going to bury my head in the sand; I don't want to do anything. Let's just ship our own laptops, our own company devices" or "Let's just force everyone to drive or fly on site." These measures incur incredible inventory management and administration costs and astronomical travel and consulting fees. If you are still using any of these measures, it's

time to replace these and to use Moving Target Defense to defend yourself against cyber threats.

Moving Target Defense Turns Your Sandcastle into a Submarine

To talk about Moving Target Defense broadly, we need to start with the idea of static defense. A good way to understand static defense is with the analogy of a sandcastle. Waves and waves of attacks come at you, so to defend yourself, you build taller and thicker walls. These constant waves of attacks come at your system to degrade your security posture. Ideally, you can create enough defenses at a fast enough pace that you are staying ahead of your adversaries. In many situations though, you're just not able to beat them. One day a strong and big enough wave will break your sandcastle, will break your defenses. You can't patch fast enough, so you experience a new Zero Day or security vulnerability that hackers can use to attack your systems. Moving Target Defense takes your sandcastle and turns it into a submarine. It’s airtight, and it's hardened. It's also proactively defending itself since it is moving away from enemy reconnaissance. Also, there’s no element of patching because it’s constantly getting updates. That way you're not worrying about whether your system is updated to the latest and greatest. You know it is.

If for example there's a virtual desktop that you're worried about, you can simply destroy it and a brand new fresh one is built from a golden image. Traffic nodes work together to obfuscate and anonymize who is connecting to your network. If no one knows that they’re connecting to a customer network, they can't begin to create an attack profile against it. And these are captured in a full software-defined wide area network (SD-WAN), so there are no longer any external interfaces available for attackers to try to exploit. And hardening your system against cyber-attacks means you’re protecting your remote connectivity as well.

Shoring Up & Securing Your Company for Remote Connectivity

Cybersecurity and remote connectivity are intrinsically connected. We need to ensure we carry out the goal of remote connectivity and at the same time, that we can work in an environment secure enough for IT compliance and security teams. But this security has

to still be fast enough for operations because remote access systems are not simply cybersecurity tools, these are efficiency tools with a critical need to be cyber secure. What does this mean? Let's look at a strict connection time, for instance an unpatched RDP server, which has a three to five second connection time. If we then start to layer in some of the cybersecurity frameworks and restrictions, remote connectivity might take 7 to 12 minutes. Possibly many of you have traveled down the rabbit hole of multiple jump posts of 16 different logins to get to one spot because it's supposed to be the most secure method. Yes, it's a potentially secure method, but operationally, it's too inefficient to be effective.

What is important is to bring down the connection time while at the same time aligning with all of the strictest cybersecurity frameworks. The goal is to reduce mean time to recovery, or the time spent getting to the problem. How to better take advantage of production data and remote connectivity to know when problems are going to happen, to see that your systems are humming along at their most efficient state? And then to get the best people to the problem faster and to record what they did.

An extremely important aspect to understand is attacks would have only worked (and did only work) when the networks had Internet access. Now, with the advent of more and more remote connectivity and with transferring data in and out of these operational networks, many companies find themselves with Internet access in places they never thought it would have been enabled. The important point is to not stick your head in the sand and go back to a siloed network to protect yourselves from attacks. There are too many operational benefits for remote connectivity, whether it be preventive maintenance, analysis of your factories' operations, centralized management, and more. There are huge economies of scale with remote connectivity, but you need to make sure you're controlling your data flows. You need to know how data is leaving your network and how people are able to get in.

Concrete Use Cases for Remote Connectivity

Three concrete use cases for remote connectivity include the following. The first is 24/7 operator access. This use case can be for your routine management and debugging. It can be that your company has a multi-facility model and A team, which is not on site. You want to get that A team to the problem faster. If you have multiple facilities, you can quickly centralize a lot of the engineering and overhead and management of distributed systems across those potentially geographically disparate locations. The second use case is vendor access for maintenance and debugging. Many companies

want to standardize this process to make it easy to control how vendors and third parties get into their networks to perform routine debugging, maintenance, patch management, and emergency access to fix a problem. You need to get vendor experts into your OT network quickly and securely while your systems are locked down to allow exactly what the vendors need to do for exactly as long as they need to do it. This puts you in control of how third parties are entering your networks with the ability to fully audit and record for auditing or training purposes. The last use case is secure data streaming. You need to effectively anonymize where that traffic is coming from, so you can gain the element of obscurity in addition to the full end-to-end encryption that is what you would expect in data streaming.

Learn More About Building Cybersecurity Defenses

There is a lot more to talk about when discussing cybersecurity and remote connectivity. A lot. The points I reviewed above in addition to the security features built into the ICONICS platform and different measures you can take to secure against cyber threats were discussed in the ICONICS ***Transform 360*** webcast "Hardening Your System Against Cyber Attacks". Presenters also provided a demonstration on secure remote connectivity to put these points into perspective. The presenters, all experts in the field, included Oliver Gruner, ICONICS Corporate Account Director for Mitsubishi; Yuki Shimizu, Engineering Manager from Mitsubishi Electric Automation; and Ben Burke, **Dispel** Chief Operating Officer. (Read more about Dispel below).
The time is now to understand the urgency of cyber threats and to take actions to defend against them. Just like you would do when you are traveling. You don't stay home because there are pickpockets, and there's a chance you will fall victim to such a crime. You take the necessary precautions to minimize your chances. It's just plain good sense.

ICONICS and Dispel are here to help and guide you. You can learn more about building cybersecurity defenses that work by watching the "**Hardening Your System Against Cyber Attacks**" webcast.

A Bit of Background about Dispel

Founded in 2014 and built out of the broader military industrial complex, Dispel provides a remote access tool for industrial networks. The company was the first to bring moving target defense to the commercial marketplace with a specific aim towards remote connectivity in critical or operational environments. Simply put, the company builds secure remote access for OT environments with next generation moving target

techniques in the manufacturing, oil and gas, water, wastewater, chemicals, and other broader OT sectors. Moving Target Defense or MTD is not new; in fact, it is a well-known topic that's been asked for over a decade by the Executive Office of the President. Its goal is to increase complexity and cost for attackers, to limit the exposure of known vulnerabilities, and to remove the opportunity for attack wherever possible. All of these security aspects come together to increase system resiliency. In short, the goal is to make it harder for attackers because they're not going to waste money and time trying to attack you. From a military science standpoint, the goal is to make the intelligence gained by adversaries useless, so they are forced into bad attack positions.

Written By:
Mary Anne Ballouz,
Marketing Communications Writer