One Step Ahead:
Emerging Cyber Security Trends & How to Prepare

by Daniel Lindley

One Step Ahead:
Emerging Cyber Security Trends and How to Prepare

By the time you have finished reading this sentence, multiple cyber-attacks will have been launched internationally. The biggest mistake you can make when it comes to cyber-attack prevention is assuming that your network is too small to matter to hackers. The reality is that attacks are often opportunistic and small networks may be compromised as a result of having too little protection while larger networks may be better protected in many cases. They just tend to make for bigger headlines when they are compromised.

As recent high-profile breaches such as the CDK ransomware hack have shown, the consequences of being caught off-guard or underprepared for an attack can be vastly detrimental. The attack affected 15,000 businesses and cost $1 billion in business losses as a result. Ransomware installation can come in from many avenues including phishing emails or device vulnerability exploitation.

Recently, U.S. investigators have discovered a hacking campaign, named “Salt Typhoon,” where hackers linked to the Chinese government have gained access to a handful of U.S. internet service providers. Unlike the similarly named “Volt Typhoon,” which appears to be focused on gaining access to networks to launch later cyber-attacks. Salt Typhoon seems to be focused on gaining intelligence information and is further proof that critical infrastructure is a major target of malicious agents.

Projections from Forbes Advisor:

The **cost** of damage incurred by cybercrime

is expected to reach

$10.5 trillion

by 2025

That’s about

$32,000 per person

in the U.S.

Cyber-attacks are occurring more frequently and with such swift advancements in technology, they are only gaining momentum. Additionally, on top of customer data and safety compromised, the financial repercussions can be impossible to recover from.

Through witnessing impacts such as the one felt by a town in rural Texas that experienced attacks on their water systems, we are learning just how far a cyber-attack can go. These attacks continue to demonstrate the importance of having and utilizing cybersecurity and incident response plans, hardening your network, installing server backups, acquiring cybersecurity insurance, providing security awareness training for your entire team, mastering vulnerability management and managing third-party relationships.

> **There is an unspoken myth in the industry that large companies carry the target on their back.**
>
> **But what's the truth?**
>
> **Small, family-owned companies are just as susceptible to a cyber-attack as any large carrier.**

The CrowdStrike patching incident shed light on other potential weaknesses in a cyber response plan. This incident occurred during a faulty update and happened while following standard procedure, leading to one of the largest outages in IT history with roughly 8.5 million systems crashing. The crash caused an estimated financial damage of $10 billion (about $31 per person in the U.S.). Even with system practices being followed, numerous companies were significantly impacted by the faulty third-party update, stressing the importance of third-party relationships, vendor due diligence, and incident response tests in preparation of actual incidents.

The size of your company does not make you immune to attacks and thinking this way can make you vulnerable if you don't take certain measures to protect your data and empower your staff. Hackers often see rural ISPs as targets, assuming they lack the resources or expertise to defend against sophisticated attacks.

Within minutes, hackers can gain access to critical systems including your customer database, billing platform, and even core network routers. Communities put their trust in you as their provider to keep them connected to healthcare, education, work, and each other. To keep your network secure and your community's trust strong, the following steps can be the difference between protecting your data and leaving it vulnerable.

Put a Plan in Place

A critical step towards network security starts with your Incident Response Plan (IRP). It's imperative to incorporate this plan into your daily business operations. This isn't a binder to sit on a shelf and collect dust; your team should feel comfortable with the contents of your Incident Response Plan and play an active role in building out your defense.

Providers with an active IRP in place can overcome attacks more efficiently than providers that are either unfamiliar with theirs or do not have one at all. Instead of wasting time figuring out their next move in a way that is frantic and scattered, our providers with an IRP have a playbook to follow.

To assess network strength, we conduct vulnerability assessments, social engineering campaigns and tabletop walk-throughs for providers looking to test their current protective measures and IRPs. These cyber drills are simulations that mimic real-world cyber-attacks. The experience is valuable to providers as they navigate their approach to safeguarding their network and knowing how to react if an attack does occur.

Don't Miss Out on Your Funding

With BEAD being top of mind, it's important to consider your cyber plans as you prepare for the pre-qualification process.

If you're finding yourself stuck, the walk-through can also highlight areas that need revisiting to remain cyber complaint.

Empower Your Team

Human exploitation is one of the most common causes of cyber-attacks. Someone clicking a malicious link can be a painful reminder that regardless of the technology you have in place, people can still open the door to cybercriminals if they are not given the tools to identify and avoid attack.

Your employees stand on the digital frontlines and can be one of your greatest tools in preventing an attack if given the proper awareness and training. Through Security Awareness Trainings, your team should be educated on topics such as phishing scams, password security, and best practices overall. This step alone will significantly reduce the chances of a breach.

Additionally, assessing the cybersecurity practices of your third-party vendors and partners before signing any contracts is another key factor in relationship management. Regularly auditing your vendors helps ensure that external sources will not be the reason for a cybercriminal to impact you.

Monitor Your Network

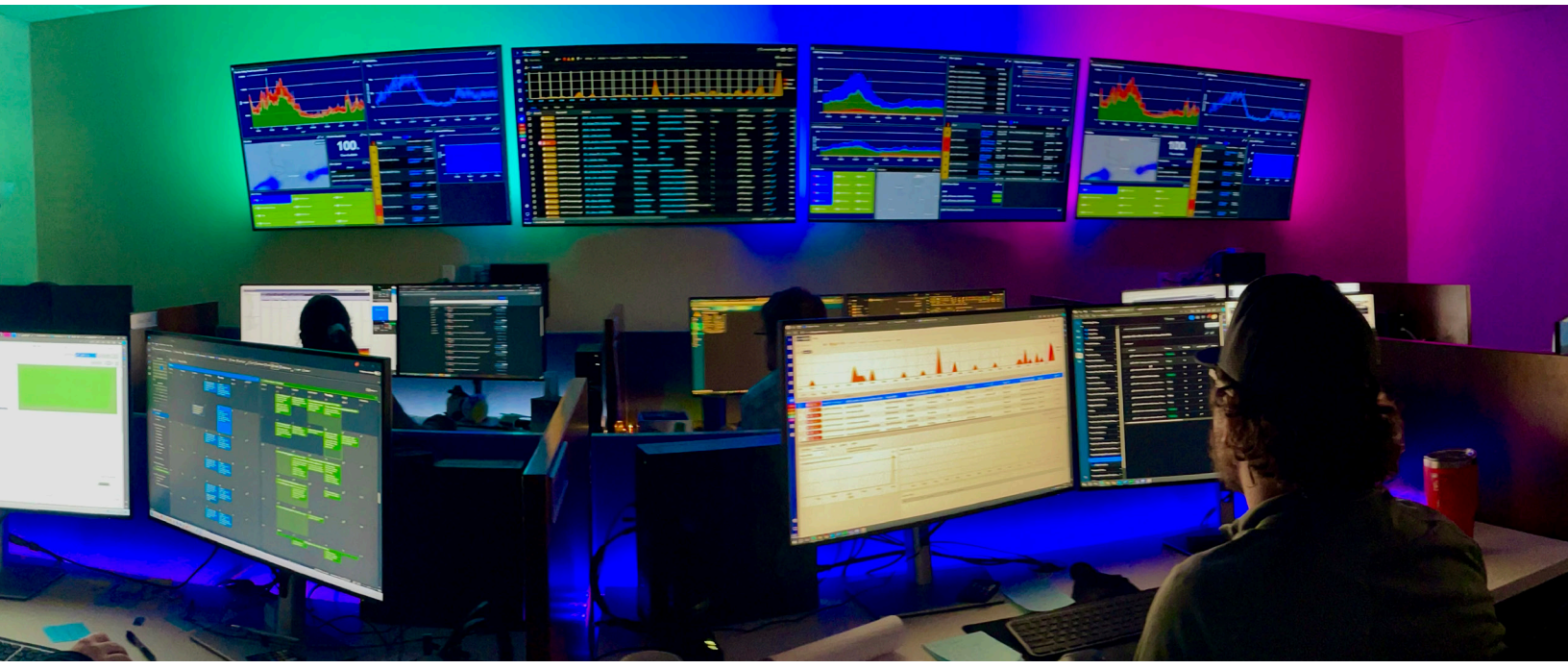
Continuous monitoring is crucial for network insight. Understanding your network activity on a regular basis gives you an advantage when it comes to detecting unusual activity early on before it has the chance to become a full-blown attack. Working with your own or JSI's NOC and security teams to employ tools such as DDoS Mitigation and Vulnerability Assessments can track network activity and alert you of any blind spots or areas susceptible to attack.

Part of the vulnerability assessment we conduct with our providers is to show them just how open their network potentially is. Seeing the exact areas of vulnerability is eye-opening to many providers that are on the fence about how far to take their protection setup.

Maintain Your Network

Daily server backups can become your best friend. While they can feel like a repetitive formality, they can become your redeeming feature amidst attack. A provider that came to us for help after they experienced an attack now maintains regular server backups. They now conduct daily server backups and know that in the event of another, they can avoid paying ransom entirely by restoring their systems and ensuring that crucial customer data and financial information is not lost.

That same provider also invested in cybersecurity insurance, something that can often be overlooked until it becomes too late. The insurance policy covers a range of costs, including legal fees notification expenses for affected customers and potential business losses due to downtime.



In Conclusion, Awareness is Key

As technology evolves, so do cybercriminal tactics. Emerging threats like artificial intelligence-driven attacks, deepfakes, and more sophisticated phishing scams mean that proper cyber-attack prevention measures should never sit still.

Utilizing experts to outsource your cybersecurity needs can give you the tools and peace of mind to ensure you are prepared for the ever-intensifying digital landscape.

Amidst the recent cyber-attacks, it is clear that the strength of your network is only as robust as the proactive steps you take to protect it. The rise in cyber-attacks, whether targeting large corporations or small businesses, highlights the critical need for comprehensive cybersecurity measures. No company, regardless of size or location, is immune to the evolving threats in today's digital landscape.

By implementing strong security measures, you can safeguard not only your network but the trust and well-being of the communities you serve.

About Daniel Lindley

Daniel Lindley is JSI's Senior Cybersecurity Specialist and is based in Lubbock, Texas. His cybersecurity expertise includes the following certifications: CISA, CISSP, HCISPP, Network+, and Cybersecurity Fundamentals. Prior to joining JSI in 2021, Daniel was an IT auditor for nearly seven years, serving as an Information Security Officer for the last two years. Before his career in IT, Daniel worked in a state crime laboratory for more than nine years, performing serology and DNA testing on evidence and testifying on evidence in court. Daniel has a bachelor's degree in Cell and Molecular Biology and a master's degree in Pharmaceutical Sciences with a concentration in Forensic Serology and DNA.