The Cyber Threat Survival Guide: How to Prepare for Future Hacks
The cyber space is wild. It’s always changing, always evolving, and always posing threats - whether you know it or not. Similar to how you can’t predict for a bear or snake encounter in the wilderness, you can’t predict the types of threats your organization faces on a daily basis from cyber criminals.

**But you can prepare.**

It’s time to shake up your strategy and prepare for the emerging threats that come with an evolving digital landscape. In this “survival guide,” we’ll walk through how to recognize risk and prepare for the expanding threats that will shape cybersecurity in the years to come.
First, let’s take a look at the major social and professional shifts that introduced the new challenges we will face.

**WORKING FROM HOME BECAME THE NORM**

In the throes of the pandemic, employees went home to work, and remote access quickly became precedence for IT teams. Systems and information that were solely accessible on an organization’s network now had to be accessible to employees essentially anywhere. As more employees accessed their company’s network through remote access tools like VPN, entryways into internal systems weren’t protected by office walls. Thousands of new avenues into organizational networks were opened via remote access connections, and hackers took notice.

**CYBERATTACKS SURGED**

Incidents of ransomware surged to 158% in North America from 2019 to 2020, and hacks aren’t stopping any time soon. Hackers released insidious ransomware posing as COVID-19 contact-tracing apps to prey on people looking for answers during the initial surge of the pandemic. Cyber criminal groups have wreaked havoc on supply chain organizations through ransomware efforts. Phishing campaigns were launched that hijacked brand names to get the attention of employees and third parties alike. Organizations suffered financially and reputationally, and already overwhelmed teams were further exhausted.

**BUSINESS CONTINUITY AND DISASTER RECOVERY (BCDR) WAS REPRIORITIZED**

While many organizations are good at planning for small-scale IT disasters like the loss of a single site or database failure, there was no precedent or preparation for the shift to virtual workplaces when offices were closed and employees began working from home full-time. Systems melted down as VPNs designed to handle 10% of the workforce were pushed to 95% capacity. Organizations of all shapes and sizes had to figure out remote employee access on the fly.
### SolarWinds
Malicious code was encrypted into a routine software update and distributed to 18,000 SolarWinds customers.

Lessons learned:
- Hackers are now embracing the “hack one, breach many” mentality. If they go after one company that has ties to several other companies, they can kill two - or several thousand - birds with one stone.
- Don’t ignore the signs. A few companies and security teams noticed quirks in the software update, but didn’t report them.
- Oversharing is not always smart marketing. The SolarWinds website had a detailed list of its Orion software clients, making them an even more appealing target.
- Don’t underestimate complex passwords. Apparently, the server password solarwinds123 was on a public message board and used in the attack.
- Companies might need to re-think the way they install software and handle updates.

### Colonial Pipeline, Co.
The nation’s largest fuel pipeline was hacked by criminal group DarkSide, shutting down fuel operations and resulting in a temporary gas shortage.

Lessons learned:
- One password is all it takes. Hackers discovered a password on the dark web that led to an inactive (but open) VPN account, which is how they got into the fuel pipeline’s network.
- Speaking of VPNs, de-provision and de-activate all VPN accounts or access points for employees who have had any change in personnel status (promotion, demotion, termination, re-allocation).
- Or, better yet, replace your VPN with a stronger alternative.
- Multi-factor authentication is necessary. If it was implemented, the hackers might’ve been stopped in their tracks.

### Kaseya
The software provider experienced a ransomware attack that inserted malicious code into its VSA software and infected several dozen managed service providers (MSPs) in its supply chain.

Lessons learned:
- All organizations NEED authentication methods. Hacking group REvil exploited authentication vulnerabilities in Kaseya’s vendor security alliance (VSA) software to compromise MSPs and demand the highest ransom payment in history.
- VSAs and remote monitoring and management (RMM) tools need to be secured. Whitelist the entities trying to access critical systems and implement a Zero Trust framework to tighten security gaps.

### JBS USA
The world’s largest meat processing plant was hit with ransomware and forced to stop meat production.

Lessons learned:
- Cyberattacks impact our day-to-day reality. JBS stopped meat production after learning about the attack and caused a temporary meat shortage and inflation of meat pricing.
- Global supply chains are among top targets for hackers due to their expansive impact. Organizations under the global supply chain umbrella must invest more in cybersecurity to prevent production-halting attacks.
- The bigger the company, the bigger the pay out: JBS paid an $11 million ransom in response to the attack.
A Survival Guide for Emerging Cybersecurity Threats

This guide is meant to advise on how to protect against cyber threats and the risks associated with remote access connectivity. This is not a comprehensive manual to secure every attack surface. It’s a tool to sharpen resilience, adopt more creative security planning, and learn from past lessons to recognize future trends.

The New Age of Workplace Cybersecurity

Returning to the office will be an adjustment for everyone, including IT security teams. What was once the chicken wire and bandaids that IT teams used to keep operations rolling amid the pandemic should now be part of new company cybersecurity protocols. Security managers will benefit from a shrinking attack surface as employees will once again reside within the corporate security perimeter. However, there are added challenges to consider.

The back-to-the-office checklist

- Map out the hybrid network – Anticipate a new normal of in-person/remote schedules. Make sure you’re clear on company policies surrounding these arrangements so you can prepare.
- Educate new (and de-programmed) employees on proper network behavior – Employees likely forgot in-house security best practices. Don’t let teams become complacent just because they can wave to their IT teams again.
- Affirm and reaffirm company policies – In order to prepare for changes, be sure to create processes that clearly outline any policy that impacts cybersecurity.
- Solidify the back-up plan – If the unpredictability of remote work teaches us anything, it’s that we need a backup plan. Make sure it’s solid, easily understood, and ready to execute when/if the time comes.

Protect Against Ransomware

Ransomware will increase and become more vicious as the “bad guys” get greedier and more innovative. Be vigilant and set the tone for the organization.

RansomWar Doctrine

- Never let your guard down - Ransomware isn’t going to subside; there is too much money in it. Always be on your guard against cyber criminals. Do all you can to secure all access points and perimeters.
- A company that trains together stays together - Malicious actors are improving social engineering techniques. Keep employees informed and savvy so they don’t get exploited.
- “Always-on” industries, always be on alert - Cybercriminals will continue to extract pain on healthcare, critical infrastructure, government services, and education. These institutions have critical access points that lead to valuable data that hackers prize. Implementing critical access management is key to protecting these networks and systems from a breach.
- Wherever there is profit, there will be an attack - Bad actors will find new sectors that are increasingly vulnerable and industries that will pay more.
- Don’t have a failure of imagination - Perpetrators have started waging mass ransomware attacks that slow response and recovery time of their victims and won’t stop. As these continue, organizations will struggle to defend multiple attack sites. Don’t underestimate the kind of mass chaos malicious attackers could eventually cause.
PREPARE FOR CYBERATTACKS 2.0

With more employees working at home, SaaS platforms have become integral to daily operations. This next generation of ransomware can spread to the cloud and result in financial costs, including ransom fees, forensics, legal, regulators’ fines, penalties, and data recovery.

Traveling to the cloud? Follow these safety tips...

• Use offline as well as online backups. Many organizations have gotten away from using tapes and offline backups, but online backups can be hacked. Use both for added security.

• Implement active monitoring to spot irregularities right away.

• Perform penetration testing. Test all buckets fully - simply restoring a file from backup is NOT adequate.

• Try threat hunting – a trusted third party will look for vulnerabilities to exploit so network managers can secure discovered gaps.

• Run incident response exercises for ransomware so the team has a rehearsed plan to limit exposure and resolve quickly.

• Educate your users. They are your best defense. In addition to training, issue frequent updates in the form of bulletins, newsletters, and emails.

Embrace more privacy laws and enforcement

WARNING: Compliance is about to get even trickier

We’re going to see more privacy laws passed and more enforcement of the ones we have. The White House released the Executive Order on Improving the Nation’s Cybersecurity that specifically calls for Zero Trust Architecture, multi-factor authentication, and increased auditing methods. Other compliance updates include an extension of the California Privacy Rights Act (CPRA) and the continuation of heavy fines from the EU’s General Data Protection Regulation (GDPR) which is based on violators’ revenue.
SECURE ENDPOINTS FOR REMOTE WORKERS

It’s time to evolve approaches to endpoint security. The name itself is a misnomer – hackers typically start with the endpoint, not the servers. They phish and socially engineer their way into access points, so a more holistic approach must be taken.

AN ENDPOINT RESET

<table>
<thead>
<tr>
<th>THEN</th>
<th>NOW</th>
</tr>
</thead>
<tbody>
<tr>
<td>A remote worker was a special case.</td>
<td>Organizations will likely have hybrid office schedules, with remote workers becoming the dominant case.</td>
</tr>
<tr>
<td>Running anti-virus provided fast detection to secure vulnerabilities.</td>
<td>Switch from relying on detection – invest in solutions that provide automated, responsive, reactive controls.</td>
</tr>
<tr>
<td>The priority is infrastructure protection.</td>
<td>Prioritize the security of data and people by adding a framework like Zero Trust.</td>
</tr>
</tbody>
</table>

RAISE YOUR IDENTITY ACCESS GAME

It’s time to stop with the spreadsheets outlining access permissions. Authentication methods and access management software are some of the most overlooked security tools. They double, triple, and quadruple check access attempts to ensure the person requesting access matches the identity of the person who has been granted access. Don’t underestimate this security practice; hackers will take advantage of the lack of access verification just when you think it’s unnecessary.

Essential protection toolkit:

- **Multi-factor authentication** – Use MFA for all access if you can. It’s a lot easier than in days past. If you’re already doing it, do more; implement it across all channels, platforms, systems, networks, and applications.
- **Privileged access management (PAM)** – Adopt a PAM tool to protect users with high levels of access. Hackers target system administrator credentials because they allow them to escalate and access an organization’s most valuable data.
- **Third-party access management** – Use a third-party vendor access management platform to maintain control over external users with privileged access.
GET SERIOUS ABOUT THIRD-PARTY RISK MANAGEMENT (TPRM)

Third-party risk management is now recommended by most regulatory frameworks, including the Executive Order on cybersecurity. Poor third-party security continues to be a contributor to major breaches around the world and organizations need to have something in place to manage third-party risk. You need to know who your third-party vendors are, what they have access to, and when they’re on your network. That requires more than reviewing third-party activity spreadsheets once a year.

Rules of engagement:

• **Inventory your third parties and vendors** – Know who they are, and keep track of critical information about employment status, leadership, reputation, policy, and practices.

• **Assess risk and rank it** – The due diligence process of evaluating and ranking risk level will emit valuable information on the company’s security standards and resources.

• **Implement extra controls for third parties with higher privilege** – Elevated credentials are what bad actors prize. Prioritize their security.

• **Use an automated access management tool for third parties** – It will allow network managers to segment by access level, monitor all activity, audit all network sessions, and manage user permissions.

BECOME MORE RESILIENT

It’s not about how hard you fall - it’s about how quickly you get back up. Prepare for the worst by recognizing all attack scenarios and identifying all security gaps, then securing all access points and endpoints.

• Think outside the box when it comes to potential cyberattacks or data breaches. If you can imagine it, it can happen. Or read some fiction and plan for a Michael Crichton scenario. Incident Response and DR/BCP testing should be creative.

• Assume you will be hacked. What’s next? You’ll need more than backups.

• Talk early and often with leadership teams and boards.
  • How would they respond to a hack/ransomware attack?
  • Would they pay?
  • Does your organization have a way to pay?

• Consider SaaS apps – they can help you scale, but secure the cloud first.
Conclusion

There are now more challenges than ever in cybersecurity, most no one ever saw coming. The key is to recognize social, economic, and environmental shifts, big and small, that will change the threat landscape for your organization - then take action.

Network protection must be more than the sum of its tools. True security requires strong leadership communication, informed and trained employees, and an imaginative security team. This survival guide is about agility and resilience that comes from constantly bullet-proofing your organization’s policies, procedures, and technologies against a range of threats - no matter how unpredictable.
About SecureLink

SecureLink is the industry leader in critical access management, empowering organizations to secure access to their most valuable assets, including networks, systems, and data. By leveraging Zero Trust principles, machine learning, and artificial intelligence, SecureLink provides comprehensive security solutions to govern, control, monitor, and audit the most critical and highest risk access points. Organizations across multiple industries -- including healthcare, manufacturing, government, legal, and gaming -- trust SecureLink to secure all forms of critical access, from remote access for third parties to access to critical infrastructure, regulated information, IT, and OT.

securelink.com | 888.897.4498 | contact@securelink.com

© 2021 SecureLink, Inc. All Rights Reserved.