Cyberwarfare in a Borderless World:
11 Tips for Ensuring Security

The expansion of the digital world directly impacts cyber risk and vulnerability. Due to cloud adoption, remote work, and other emerging practices, corporations are less protected. Without proper safeguards in place, today's businesses are at the mercy of bad actors all over the world. Cyber vulnerabilities will lead to warfare that transcends borders—and we've seen the evidence most recently in the 2022 Russian invasion of Ukraine.

In late February 2022, a never-before-seen wiper malware of suspected Russian origin targeted Ukraine's government ministries and financial institutions.[1] Fortunately, Microsoft's Threat Intelligence Center detected the malware—and Microsoft quickly developed the code needed to block the virus. This incident is one example of the growing threat of cybersecurity attacks and events in the wake of global unrest.

Today's cybersecurity leaders face a world where they cannot predict what comes next or how it will affect their organizations. Cybercriminals, hacktivists, and vandals flourish in times of instability and uncertainty—and they have the power to create worldwide chaos, unconfined by oceans and borders.

ANATOMY OF ONGOING CYBERWARFARE

The cyberattacks we've seen as part of the current Russia-Ukraine war are more destructive than generic viruses and ransomware. Since mid-January 2022, various Ukrainian companies have been attacked with deadly malware that leaves assets compromised and inoperable.[2] Some attacks have resulted in machines being erased entirely, with no possibility for ransom payment or recovery options.

Hackers have gained full control of cyberwarfare, and attacks can come in various forms. Even people who aren't intended targets can experience the fallout. As Stuart Madnick of the *Harvard Business Review* points out, attacks can be both direct and indirect.[3]

- **Direct Attacks**

  When people think of cyberwarfare, they often picture direct attacks that specifically target one entity. For example, a virus infiltrating all your organization's devices is a direct attack. These can also include phishing scams and stolen data.

- **Indirect Attacks**

  Indirect attacks happen on a grander scale because there is no individual target. Instead, the target could be a power grid, supply chains, banking systems, water treatment, communications, or transportation. These attacks often create more widespread damage due to the number of people they impact.

Cyberattacks in any form must be avoided—which means organizations need to have safeguards in place to protect from both direct and indirect consequences. As malware and hacking techniques evolve, bad actors will cause more devastation worldwide.

As we enter the era of cyberwarfare, the U.S. CISA, CERTs, and other governmental agencies in various countries have advised firms to shield up and prepare for more cyberattacks. Executives who want to see their corporations succeed must recognize the value of cyber threat intelligence, proactive risk management, tabletop exercises, and self-audits to consistently assess their ability to detect and close cybersecurity gaps.

Hackers will target anyone who is vulnerable—and anyone could be the next victim. Your organization's best way forward is to develop an end-to-end cybersecurity approach where technology and security hygiene are maintained.

Don't be reactive; take steps to protect your enterprise today by following these **11 cyber hygiene tips.**

1. Update and Patch Your Systems

Software creators are continually developing updates to fix bugs and enhance performance. While it may be tempting to ignore these updates until there's a convenient time for installation, you should always run them as soon as they're available.

For critical systems, we recommend running new updates in a test environment before deploying it to the production environment. This will confirm the effectiveness of the update without putting your operations at risk. Additionally, in some cases, patches for vulnerabilities may not be immediately available. Always follow proper mitigating measures until updates are released and replace software and devices that your vendor no longer supports.

2. Apply Strong, Multi-Factor Authentication

All systems and applications should have multiple lines of defense for login. Hackers can easily guess simple passwords with attacks like Brute Force, so enforce a complex password policy at your organization. We recommend a required combination of:

- Alphabet letters
- Numbers
- Special characters
- 12+ characters

Apply multi-factor authentication to internet-accessible accounts, administrative accounts, and critical system accounts. Using multi-factor authentication prevents attackers from gaining access through Brute Force, phishing, or other means.

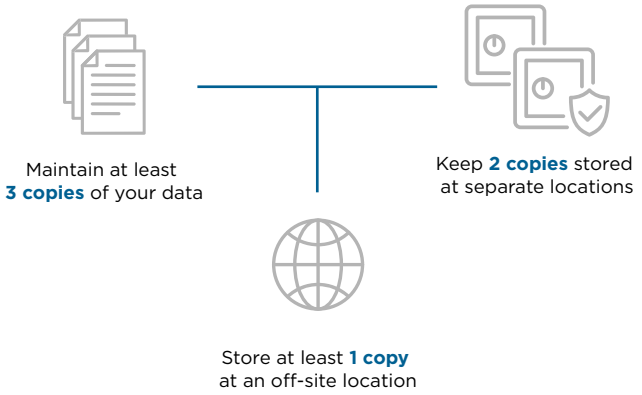
3. Back Up and Test Your Systems

If your data and systems get compromised, it's critical to have a stored backup to get everything up and running again. Carefully consider which data backups are necessary for your organization—and how long should you keep them. Additionally, test the restoration of your backups regularly to ensure your business' downtime will be limited in the event of a cyberattack.

The 3-2-1 rule can help set up your backup process. To follow this rule, keep three versions of your data (your production data and two backups) on two different media (for example, different physical hard drives), and keep one copy in a different location for disaster recovery (for example, physical). This way, you always have a way to restore your systems—even if ransomware encrypts your network.

Lastly, restrict access to your backups. Keep access rights only to those necessary and consider encrypting your backups to prevent mistaken access.

3-2-1 Backup Rule



4. Prevent Social Engineering

Attackers will use current events—such as the Russia-Ukraine war—as a distraction to covertly compromise resources or exploit news events to run social engineering campaigns. Businesses, consumers, and government organizations should exercise extreme caution during major global events.

Bad actors take advantage of people who are looking for news updates or searching for ways to help those in need. Attackers exploit humanity's urgent need for information and involvement by running phishing campaigns via SMS, email, third-party messaging platforms, and social media apps. These campaigns usually feature enticing headlines and lead to malicious websites. To prevent your teams from falling prey to these, encourage employees to think rationally while reading or responding to unknown content or unfamiliar requests.

5. Implement Logging and Continuous Monitoring

Log files play a key role in detecting attacks and handling incidents. Consider system logging, network logging, application logging, and cloud logging. What does your organization need? Is there anything you're overlooking?

Restrict access to log files and store them in a separate network segment. If attackers modify or delete the log files, incident investigation becomes impossible. Additionally, reinforce cybersecurity measures and staff during nights, weekends, and holidays. Cybercriminals often target their victims during gaps.

At SDG, we recommend monitoring your IT landscape by leveraging technologies like SIEM, XDR, and EDR and integrating them with the IOCs & TTPs shared by governmental agencies and reputed firms. We also recommend initiating proactive threat hunting on your cyber defense platforms.

6. Encrypt Storage Media

Don't let sensitive company information go unprotected. Encrypting storage media makes critical data unreadable and useless if it falls into attackers' hands. Encrypt your hard drives, laptops, mobile devices, USB devices, and anything else that stores sensitive information by using secure encryption software.

7. Segment Your Network

Segmenting your network divides your network into multiple zones and minimizes the impact of a cyberattack. It prevents malware or attackers from spreading across your entire enterprise, and it reduces the effects of DDoS attacks.

When segmenting your network, think about how the network zones are organized and connected. For example, you can define zones using firewalls, access control lists (ACLs), and data diodes. You can also choose to make a network only physically accessible as an "air-gapped network."

8. Stay Vigilant of Ransomware and Supply-Chain Attacks

Companies with heavily integrated third-party systems face a major risk of supply-chain attacks, ransomware campaigns, and extensive malware. The NotPetya ransomware attack affected the operations of many multinational companies in 2017. The attack—which was originally designed to infiltrate computer systems through a popular Ukrainian accounting software—ended up doing $10 billion of damage globally, serving as a classic example of malware's far-reaching consequences.[4]

When U.S. technology firm SolarWinds was unknowingly hacked in 2020, software updates containing faulty code enabled hackers to spy on SolarWinds' major clients, including Microsoft and top government agencies.[5] Today, the event is considered one of the most catastrophic attacks on the software supply chain.

To prevent disasters like these, organizations should review the security practices of any third-party software integrated into their infrastructure—particularly when teams operate in currently vulnerable parts of the world. If you don't have proper safeguards in place, a successful attack on a third party could make your organization the victim of collateral damage. **Are you confident in your third-party risk management plan?**

The **NOTPETYA RANSOMEWARE ATTACK** affected the operations of **many multinational companies** in 2017 and ended up doing

$10 billion

of damage **globally**.

Don't wait to test your crisis response processes in the heat of an actual crisis.

9. Control Access to Your Data and Services

Only give employees access to data, systems, and accounts necessary for performing their tasks. This limits both the mistakes a user can make and the actions attackers can perform if they gain access. Additionally, there are several steps you can take to protect your data on both a user level and a system level.

- **User-Level Protections**
  Follow zero-trust access principles with all service accounts, machine accounts, and functional accounts to protect sensitive data and prevent information from falling into the wrong hands. At SDG, we also recommend limiting the number of team members who have administrative rights and using the Principle of Least Privilege to assign role-based access control, which can make permissions management easier.

- Access to all data and services should be personal, with each employee having his or her own accounts. Establish processes for recruitment, onboarding, and termination of employees so you have a big-picture view of everyone's access levels. When you prepare to offboard employees, remove their access. Delete unused accounts and deactivate service accounts.

- **System-Level Protections**
  Connecting devices and services to the internet always poses a risk. Check which devices and services are reachable from the internet and take proper precautions to encrypt and protect them. Protective measures include using a firewall, disabling unused services and ports, and ensuring software is updated.

  To limit the risk of unauthorized access, only allow access to the internet when necessary. Place devices that can be reached from the internet in a separate network segment. Apply multi-factor authentication for accounts that can be used over the internet.

10. Establish an Incident Response Plan

Even if you've established extensive security measures, incidents can still occur—which means it's important to be prepared. Include cybersecurity incidents in your existing recovery plan. Update and practice this plan regularly.

Don't wait to test your crisis response processes in the heat of an actual crisis. Identify key contact points within your organization in the event of a cybersecurity incident or critical infrastructure disruption. Test your communication protocol (and backup protocols) consistently to avoid being left without a clear mechanism for disseminating important information. Conduct a tabletop exercise with all key stakeholders to learn how you would react if worse came to worst.

11. Stay Informed

The last—and most important—tip to follow for continued cybersecurity is to stay aware of current events. Follow the latest developments and advisories from cybersecurity agencies around the world like U.S. CISA, UK NCSC, CERTs, and others. Track their press releases and alerts to see what should concern you. Hold regular cybersecurity briefings across your teams and be prepared to act fast.

STAY AWARE OF CURRENT EVENTS

by following the latest developments and advisories from cybersecurity agencies from around the world

CONCLUSION

Recent events have proven the importance of having complete visibility of all users, devices, and networks in their interaction with corporate infrastructure and data. Looking ahead, attackers will find new, innovative ways to secretly invade the infrastructure, adopting the mechanism of phishing attacks to steal credentials, exploit vulnerabilities, or find credentials via integrated third-party systems. You cannot predict the time or origin of an attack, but by using the 11 tips above, you can increase your resilience in the face of cyberwarfare. **If you need help implementing any of our recommendations, reach out to our TruOps team today.**

TAKE STEPS TO PROTECT YOUR ENTERPRISE BY FOLLOWING THESE

11 CYBER HYGIENE TIPS

1. Update and patch your systems
2. Apply strong, multi-factor authentication
3. Back up and test your systems
4. Prevent social engineering
5. Implement logging and continuous monitoring
6. Encrypt storage media
7. Segment your network
8. Stay vigilant of ransomware and supply-chain attacks
9. Control access to your data and services
10. Establish an incident response plan
11. Stay informed

ABOUT SDG

With more than 30 years of experience partnering with global enterprises on complex business and IT initiatives, SDG is a trusted provider of advisory, transformation, and managed services. The firm empowers organizations to strengthen cyber resilience by integrating AI into identity, threat, and risk management solutions that protect digital assets and deliver measurable business value. Learn more at www.sdgc.com.

RESOURCES

1. https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html
2. https://www.cisa.gov/uscert/ncas/current-activity/2022/01/16/microsoft-warns-destructive-malware-targeting-ukrainian
3. https://hbr.org/2022/03/what-russias-ongoing-cyberattacks-in-ukraine-suggest-about-the-future-of-cyber-warfare
4. https://www.brookings.edu/techstream/how-the-notpetya-attack-is-reshaping-cyber-insurance/
5. https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

SDG

Contact Us: solutions@sdgc.com

- 55 North Water Street
  Norwalk, CT 06854
- 203.866.8886
- sdgc.com