ZURICH

Cybersecurity Preparedness Checklist

Created with insights from Zurich's cyber risk specialists, this tool can help ensure your organization has the protection it needs from cyberattacks

As cybersecurity threats grow more sophisticated by the day, organizations must become equally sophisticated in their approaches to defend against them. With the right tools, training, and tactics, Zurich can help take your security to the next level – ensuring that your employees, customers, and stakeholders alike can navigate through an attack.

Created specifically for business leaders and based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework, this checklist from Zurich's cyber risk specialists outlines actionable ways to enhance your digital security across your organization.

1. Identify

What are you trying to protect? Determine which processes, systems, and data are most at risk and implement the following measures to help keep them safe.

- ○ Form an enterprise security team distinct from IT to actively fend off threats, monitor the cyber landscape, periodically review programs, and continuously test and update your policies. If you're unable to build a dedicated group, consider a Zurich Cyber Insurance Policy – Concierge Suite.
- ○ Conduct a cybersecurity risk assessment to evaluate existing safeguards and identify any holes that require immediate attention. Be aware of all devices that are connected to your network at any given moment.
- ○ Establish a formal reporting process between cybersecurity and business leadership to discuss regulatory updates, vendor agreements, security strategies, roadmaps, trainings, and budgetary needs.
- ○ Create an inventory of all assets (including hardware, software, and data) and rank them according to their associated risk and confidentiality level. Make sure any identifiable information, such as health data, can be easily modified or deleted to comply with data privacy legislation.
- ○ When onboarding vendors, thoroughly vet their security practices before sharing information with them. Consider diversifying your vendor base to mitigate impact if a particular vendor's security is compromised.

2. Protect

After identifying critical assets, move to reduce the likelihood and impact of a potential breach.

- ○ Invest in software, such as firewalls and intrusion detection to protect networks and devices and be sure to keep it updated.
- ○ Require access controls, such as complex passwords and multifactor authentication (MFA), that challenge users to identify themselves when attempting to log onto a network, no matter where they're logging in from. Only grant users the necessary access required to perform their specific job duties.
- ○ Back up mission-critical data in air-gapped, off-site data stores unconnected to your network. This also means they can be used to restore data in the event of fires, floods, glitches, or hardware failure.
- ○ Regularly test your security defense to see if it can withstand an aggressive attacker and ever-evolving threats. If you see any vulnerabilities, patch them immediately.
- ○ Conduct mandatory cybersecurity training and simulation exercises for employees during onboarding and throughout the year to ensure they're aware of emerging threats, scams, and phishing attempts.

3. Detect

Once you've established your defense, implement systems that detect attacks and negate them before they can do harm.

- Whether in house or through an external provider, invest in a 24/7 continuous monitoring service with a dashboard feature that immediately relays anomalies to responsible personnel.
- Use a security information and event management (SIEM) tool to log data from all devices on your network, using automated analysis to spot anomalies and trigger appropriate responses.
- Establish a vulnerability management program that requires (at a minimum) monthly internal and quarterly external network scans.

4. Respond

If you detect any unusual activity, act fast to isolate and mitigate the threat.

- Create an Incident Response Plan (IRP) that explains how to identify, contain, and eradicate common cybersecurity threats and includes important contacts and recovery steps. Keep physical copies of the playbook readily available in the event of a network failure.
- Prepare a documented process that manages crisis communications to employees, customers, vendors, and the public. Make sure any communications are approved by leadership and delivered by authorized officials.
- Analyze the incident to understand the threat's full potential and document triggers for future reference.

5. Recover

Even the best defense may crack when hit with an especially advanced cyberattack.

- To rebound quickly and resume operations in full, have a recovery plan ready to go. Develop a Disaster Recovery (DR) plan for all major systems based on each one's impact on the business. Include Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) that establish target timelines for when systems and processes will be restored so that you can minimize downtime and data loss.
- Test recovery plans as often as possible and stage outage drills to get an accurate sense of the organization's ability to recover.
- Conduct a risk management review after the event, noting key takeaways and lessons learned to continuously improve your cybersecurity resilience.

6. Govern

Take a proactive approach to cybersecurity governance by establishing clear policies, roles, and responsibilities that are aligned with your organization's overall risk management framework.

- After you've developed your cybersecurity objectives in the context of your business missions, goals, and stakeholder expectations, communicate the comprehensive cybersecurity strategy, ensuring it integrates with enterprise risk management and supply chain processes.
- Assign specific roles and authorities for oversight and create documented policies and procedures to guide daily operations and strategic decisions. Regularly review and update these policies in response to evolving threats, business changes, and regulatory requirements.
- Monitor the effectiveness of your governance program through audits, risk assessments, and ongoing stakeholder engagement. By embedding cybersecurity into your organization's culture and leadership agenda, you ensure resilience, accountability, and sustained protection across all business functions.

For more insights and tools to help build a robust cybersecurity program visit https://www.zurichna.com/knowledge/topics/cyber.

Zurich | 1299 Zurich Way, Schaumburg, IL 60196-1056 | 800 382-2150 | www.zurichna.com

A1-P1127878-A (12/25) P1127878