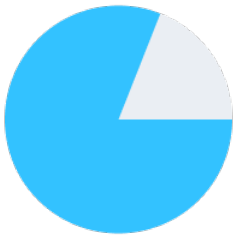
CORVUS

How Tech Companies Can Cover Their Security Bases: Five High-impact Practices

The threat of ransomware is persisting, and we continue to see attacks launched on organizations of all sizes and industries. **The tech sector has a specific draw for threat actors, where companies have rich data and downstream customers, creating opportunities for large ransom payments.** Business leaders often feel that, with the never-ending stream of news and changing advice, the biggest hurdle is determining how, and where, to start with protecting their own and their customers' IT systems.

Based on the experience of our Risk + Response team working with technology and professional services firms, **we've highlighted some go-to solutions for covering your security bases:**

At Corvus, our **Risk + Response experts** work with policyholders and cybersecurity partners to implement measures that **mitigate risk** for their organizations, including with Smart Tech E&O policyholders.



81% of data breaches
in recent years are attributed to password compromises

1. Multi Factor Authentication

When it comes to a high impact, relatively low effort security control, multi factor authentication (MFA) is top of mind. It's a crucial step for helping to prevent unauthorized access to your company (remote access) and your data (company email, SaaS / cloud applications). When implemented internally, it can help slow attackers from progressing further in your systems and help limit unauthorized access, especially when implemented for admin credentials. In recent years, password compromises have accounted for **81 percent of data breaches**, which is why MFA is often one of our first recommendations to protect your organization.

2. Endpoint Detection and Response

While antivirus software can battle low-hanging fruit, EDR functions as higher-level protection against advanced and emerging threats. With ongoing visibility and advanced monitoring for all of your endpoints, it can quickly pinpoint activity with characteristics of common attacks, and provide forensic teams with more data to ultimately limit downtime in the event of an incident.

The right EDR solution deployed properly provides **one of the best return on investments** for securing your endpoints.

3. Backup and Recovery

During a ransomware event, recovery can be complex, expensive, and time-consuming. Ransomware threat actors will actively seek out your backups in an attempt to delete them. If you don't have a robust backup solution with protective controls, offsite backups, and you've never tested them — a ransom payout may feel like the only option to resume business operations as normal.

To avoid that worst-case scenario confirm:

- your organization's backup strategy includes all of your critical systems
- your local backups are secured
- you have offsite backups
- know how quickly you can restore all of those systems

Preparation here can mean a world of difference in your response strategy.

4. Incident Response Plan & Vendor Management

An incident response plan (IRP) means your organization has a system in place before there's a security incident, so you can respond quickly and with intent. It's clear who's in charge, team expectations, and what your process is.

The incident response process can be a mad dash or scramble - having a known and tested IRP before everything is on fire can help reduce stress levels in a very stressful situation.

5. Insurance Coverage!

Insurance is a crucial step for protecting your organization and transferring risk *(we don't just say that because we love insurance — promise!).* Beyond the obvious financial safety offered by insurance, when it comes to cyber risks the relationship between an organization and their carrier should be seen more as a partnership, where **your insurance provider shares data reports and services as an ongoing source for risk mitigation.** For tech companies, a Tech E&O policy that includes fully-fledged cyber liability *(first and third party)* coverage is more critical than ever.

Introducing Corvus vCISO Services

To highlight an example of how the collaboration between insurer and insured works, Corvus offers **vCISO Services**, which is a collection of consultative services with our security partners.

The goal is to make all these decisions easier *(and cost-effective)* to strengthen their systems against cyber-attacks.

About Corvus

Corvus is reimagining commercial insurance for a digital world by making insurance smarter, companies safer, and brokers more successful. Corvus empowers brokers and policyholders with actionable insights to mitigate complex risks and reduce losses through the CrowBar digital platform, smart insurance products, and premier risk management services. Corvus is the world's largest specialty commercial InsurTech company.

Resources:
The Importance of Multi Factor Authentication in Cybersecurity (Veridium)