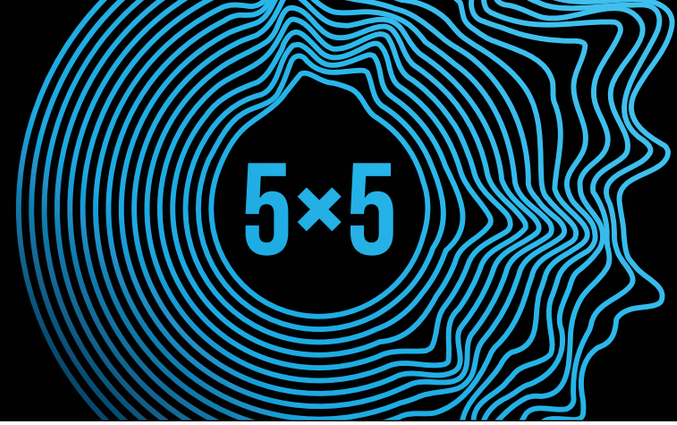
Deloitte.

COVID-19 5x5 series: Insights and actions

Cybersecurity and privacy



There's limited precedent into how COVID-19 will impact the technology-reliant business world today. Unlike past epidemics, COVID-19 has caused discrete financial "shocks" and broader day-to-day disruption, which will likely lead to secondary and tertiary cyber implications. A strategic approach will support an organization to proactively address cyber challenges during this and future extraordinary events ranging from securing remote work infrastructure, combatting fraud, preventing unintentional or malicious insider threats, and beyond. This quick summary provides some cybersecurity and privacy business insights and actions you can take today in response to the pandemic.

5 insights you should know

Increases in COVID-19–themed social engineering, phishing, and malware attacks contribute to heightened threat levels and may contribute to **delays in detection of malicious activities and difficulty in responding to these security events.**

Rapid adoption of remote work tools and infrastructure may lead to relaxed security controls; similarly, disruptions to third parties and contractors could **make safeguarding data and privacy difficult—unknowingly compromising sensitive information.**

The use of personal devices and nonsanctioned applications (Shadow IT) by employees working remotely can lead to a significantly **increased risk of cyber adversaries accessing internal infrastructure** where data and intellectual property (IP) can be accessed.

There's been a surge in requests for remote desktops. Some organizations are realizing that their **remote access may not be built to scale** and, in some cases, user access controls may be compromised.

Unfortunately, one of the many impacts of a crisis is the disturbances to normal business operations and demand, forcing **reorganizations or widespread employee cuts, which can contribute to greater risks of insider threats.**

5 actions to take now *(click link to learn more)*

1. Organizations should focus on **updating their security monitoring** use cases to generate relevant alerts while extending their threat detection and monitoring capabilities to include remote devices.
2. Review technical **data protection and privacy mechanisms** to confirm they are updated and implemented; educate employees and raise awareness of privacy and data protection practices under new working circumstances.
3. If they haven't done so already, organizations should establish guidelines for their expanded remote workforce and configure **application security and secure virtual private networks (VPNs) for remote device access.** Security operations teams should consider performing proactive scanning and implementation of greater security controls to prevent unauthorized device and application use.
4. Organizations should keep a pulse on potential threats, deploy **secure remote provisioning, privileged, and multi-factor authentication (MFA)** for high-risk applications.
5. Organizations may consider updating their security architecture and confirming coverage for a **strong risk-based insider threat monitoring program** to bolster their security in high-risk areas and provide long-term IP and brand protection.

Connect with us

COVID-19 related inquiries? Email
USCyberCoronavirusResponse@deloitte.com

Deborah Golden
Principal, US Cyber Risk Services Leader
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Jason Frame
Managing Director, US Cyber Risk Services
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Hallie Miller
Manager, US Cyber Risk Services
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP