CYBERSECURITY IMPLICATIONS OF COVID-19

Bill Stewart, Julien Bonnay, Alex Donovan, Tim Sheng

The massive shift to remote access technologies precipitated by the COVID-19 pandemic has highlighted how critical it is for leadership to adapt to evolving demands and respond to emerging security risks during a crisis. Effective leaders must understand how their role has changed in light of this pandemic and take critical steps both immediately and post-crisis to strengthen their security posture.

PANDEMIC SITUATION SUMMARY

The sudden global outbreak of COVID-19 and the ensuing healthcare crisis has forced financial institutions to adapt quickly to new work-from-home (WFH) arrangements. This accelerated adoption of remote access technologies required the creation and modification of IT infrastructure while minimizing business disruptions. Some organizations struggled to deploy required remote access technologies such as VPNs or bank-issued devices within the compressed timeline, and many firms did not fully anticipate the impact of an entirely remote working scenario for sustained periods. Additionally, this rapid transformation has exacerbated risks to the confidentiality, integrity, and availability of key data and systems, which now must be reconsidered.

Unfortunately, threat actors have not ceased malicious activity and are even crafting campaigns to target vulnerabilities on remote access platforms. Coronavirus-themed attacks on newly vulnerable infrastructure and ill-prepared staff have increased markedly. In short, cyber risks have heightened due to rapid operational changes, including:

- Organizational functions rapidly transitioned to remote operations, creating modified attack surfaces and altered risk profiles
- Security tools quickly extended to broader audiences (e.g., VPN licenses for all staff), leading to increased risks, particularly if tools are not properly configured, sized, and used
- Staff adopted new ways of working without a deep understanding of security implications, inadvertently creating security gaps and becoming increasingly susceptible to coronavirus-themed social engineering scams
- Operational expediency and continuity of operations temporarily prioritized over security, resulting in reduced defense due to configuration shortcuts or insufficient end-point solutions

CIOs and CISOs have the opportunity to learn from the pandemic and look to build a more resilient organization in the future.

SECURING THE NEW NORMAL

Technology leaders must be proactive in securing the new normal to counter the evolving threat and risk landscape. CISOs should perform a comprehensive review of all changes made against a pre-pandemic baseline, including configuration changes, device deployments, application access, elevated privileges granted, etc. Reviewing this detailed list will help identify exactly what should be rolled back and what should be kept. Policies and controls should then be updated accordingly. This will help to identify any new safeguards or tools needed to monitor the changing behavior patterns and shifting attack surfaces. Employee training and onboarding materials may also need to be refreshed to align with new remote working expectations and security tools. This comprehensive review will enable CISOs to take stock of all the changes that were made in response to COVID-19 and realign the firm's security posture as needed.

BUILDING A MORE RESILIENT FUTURE

Moving forward, a more resilient operating model must become a top priority for CISOs—smart leaders know that COVID-19, though unique, is not the last disaster firms will face. Proactively capturing and reflecting on lessons learned now will make the business more prepared for the next pandemic, cyber-attack, or other significant environmental changes. Any challenges or business disruptions faced during the transition to remote working should be analyzed and used to update business continuity planning. Incident response and crisis management plans should be tested against an expanded set of cyber risks and threats highlighted during the pandemic. Key third parties should also be reviewed in terms of what kind of security measures they deployed and how resilient their operational model proved to be during the crisis. The use of wargames, tabletop exercises, and worst-case scenario analysis should help incorporate the lessons learned during COVID-19 to prepare for the future.

ADDRESSING CRITICAL SECURITY GAPS IN THE NEW ENVIRONMENT

More immediately, technology leaders need to address critical security gaps and restore cyber hygiene to transition the business back to a semblance of normalcy from the current crisis mode. Capco recommends a quick security review in the short-term to understand changes made to the operational environment and the new risks that have emerged.

Asset criticality should be validated to identify any changes to the firm's crown jewels as a result of the new environment. Exposure to new risks need to be assessed by analyzing threat intelligence for actionable relevance to the business. Increased risk exposures should be prioritized to allow for the optimal and immediate deployment of limited security resources.

Gaps in the security program's ability to address these risks must be identified in the current state by reviewing the following:

- Applicability of security policies,
- Adaptability of processes and governance in the new environment,
- Staff security awareness and responsiveness to staffing shortfalls, and
- Ability of security technology to scale and respond to a new attack surface.

Finally, a mitigation plan should be defined to prioritize initiatives for quick deployment to restore the status quo of the security program and maintain the necessary vigilance against cyber threats.

GET IN TOUCH

Discover how Capco can partner with your business as a trusted advisor to navigate through these uncertain times:

Julien Bonnay, julien.bonnay@capco.com

Bill Stewart, william.stewart@capco.com

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at www.capco.com, or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

WWW.CAPCO.COM

CAPCO

THE FUTURE. NOW.