Remote Work **Security Assessment**

Reduce the Security and Business Risks of a Remote Workforce

The new world of remote work has created both increased security vulnerabilities and increased threats from bad actors. According to William Altman, Senior Analyst at the Global Cyber Center of NYC, "Organizations of all kinds are facing an uptick in email-based threats, endpoint-security gaps, and other problems as a result of the sudden switch to a fully remote workforce."[1] Bitdefender research reports 86% of information security professionals admitted that attacks were on the rise during the COVID-19 pandemic, with phishing and whaling recording the highest spikes in activity.[2]

Organizations had not planned to move their office workforces to remote working, and IT departments were unprepared for transitioning a workforce while still ensuring security and compliance. Nevertheless, IT teams had to enable nearly all their office staff to work remotely, sometimes with only a few days' notice and little to no planning time. As a result, this quick shift happened in emergency mode.

Under pressure to keep organizations functioning, many made operational compromises. Hard decisions were faced, and security measures were relaxed to enable employees to work remotely. Simultaneously, bad actors have dramatically increased activity. The rates of increase for the most common cybersecurity risks increased by over 30% during the first part of 2020.[4]

This unexpected and unplanned shift to remote work has resulted in a dangerous perfect storm of security risk:

- A much larger security perimeter and increased threat surface to monitor and protect
- Substantial increases in bad actor activity, such as phishing and ransomware
- More demands on IT to support and enable a remote workforce

Security teams are now challenged to reduce risks and adapt security measures to avoid social media and chatbot threats, and breaches from phishing, whaling, and ransomware. Increased remote work exacerbates threats from inadequate laptop security, personal devices use, remote access methods, and home networks.

A Risk-based Action Plan to Protect Your Organization from Remote Work Security Risks

IT organizations need to understand the current vulnerabilities in their distributed workforce and execute a risk-based approach to protect their organizations.

50% of information security professionals reported they had no contingency plan for a situation that would have resulted in employees working from home. [3]

Organizations with between 500 and 1,000 employees had an average data breach cost of $2.65 million, or $3,533 per employee. [5]

In March 2020, ransomware attacks increased 148% over baseline levels from February 2020.

The Flexential Remote Work Security Assessment evaluates and provides organization-specific security recommendations for meeting compliance and regulatory requirements, closing gaps, and reducing risks in:

- Remote access methods
- User authentication methods
- Endpoint protection
- Encryption methods
- Business-critical systems security
- Incident response plans

The Remote Work Security Assessment provides a roadmap to strengthen security and reduce the risk of breaches and data loss, as well as the resulting recovery and remediation costs, PR damage, lost business and lost customers.

Customers receive a detailed risk-based report which includes:

- Organization-specific IT security recommendations for protecting a remote workforce
- Recommendations prioritized by criticality, cost to implement and time to implement
- Guidance for security controls
- Technical details for system administrators to use as a risk mitigation guide

Organizations have entered an age of distributed work and, at least temporarily, a remote-first workforce strategy. IT security needs to match this new reality.

"Working from home is going to be a long-lasting reality within many organizations, and the security assumptions we once relied on in our traditional offices may not be enough as our workforce transitions to new, less controlled surroundings. Organizations need to use a risk-based approach with work-from-home models, then reassess and build from the ground up."[8]

Charles Henderson
GLOBAL MANAGING PARTNER AND HEAD OF IBM'S X-FORCE RED

74% of organizations report having either ad-hoc, inconsistently applied, or non-existent security plans. [6]

53% of newly working from home respondents use their personal laptop and computer to conduct work from home.[7]

Features

- Highly certified security experts
- Stakeholder interviews and technical reviews
- Review of compliance and regulatory requirements
- Assessment of critical vulnerability areas
- Risk-based security recommendations
- Prioritized action plan with remediation guidance
- Professional project management

Benefits

- Documented remote workforce security plan
- Risk-based action prioritization
- Remedies for risks from the shift to remote work
- Addresses compliance and regulatory security

1 Beware: Remote Work Involves These 3 Cyber Security Risks, April 2020

2, 3, 4 The Indelible Impact of COVID-19 on Cybersecurity, Bitdefender, June 2020

5 Ponemon Institute: Cost of a Data Breach Report 2019

6 BM Study: Security Response Planning on the Rise, June 30, 2020

7 Work from Home Study, Morning Consult & IBM Security, June 2020

8 IBM Security Study Finds Employees New to Working from Home Pose Security Risk, June 22, 2020

ABOUT FLEXENTIAL

Flexential empowers the IT journey of the nation's most complex businesses by offering flexible and tailored solutions in colocation, cloud, data protection, managed and professional services. The company builds on a platform of three million square feet of data center space, in 20 highly connected markets and the FlexAnywhere™ 100 GB private backbone, to meet the most stringent challenges in security, compliance and resiliency. Visit www.flexential.com.