RESILIENCE BAROMETER 2020

Build resilience. **Protect** value.

EXPERTS WITH IMPACT

FTI CONSULTING

Cybersecurity: Resilience requires proactivity

The complex and ever-changing nature of cyber risk requires a continued evolution in how organisations approach resilience. No longer is access constrained to the four walls of an organisation. Any connected entity can serve as a point of entry, including third-party vendors who act as a "back door" to larger enterprise networks. Responding effectively to cyber risk requires proactive and holistic management helping mitigate threats, reduce downtime, and protect an organisation's reputation.

"A cyber breach is a matter of "when" and not "if." You can't control the timing, but you can get ahead of the threat by preparing your defence. Developing a plan involving your people, processes and technologies for when that moment arrives is key to achieving cyber resilience."

JOSHUA BURCH
Senior Managing Director
Head of Cybersecurity, EMEA

The cyber risk landscape is dynamic and fluid, leaving organisations with stagnant policies and procedures vulnerable to attack. Just as threats increase in sophistication and malicious actors learn to bypass protections, organisations must continually assess and modify their cyber resilience methodology to keep pace. Our research shows that at least one in four G20 organisations have experienced a cyber attack, where assets were stolen or compromised, in the last 12 months, emphasising the need for improved security.

Further examining those negatively impacted by cyber attacks, lost revenue, reputation damage, and lost customers were the top three impacted areas. A single cyber incident can tarnish how an organisation is publicly viewed, especially if the situation is not managed carefully. However, proactive reputation management and transparency with the public can leave an organisation in a better light post-incident, instead of succumbing to the potentially long-lasting negative effects that often are associated with a breach.

Our research shows that social engineering – including phishing – is the most common attack vector, with 27% of large companies researched reporting being negatively impacted as a result in the past 12 months. These incidents do not occur in isolation. Over a third of organisations who have been impacted by a loss of customer/patient data have also lost third party information and have been victims of phishing/social engineering.

The cascading effects of a cyber attack increase the potential damages and fallout organisations face from being unprepared. Resilience requires a complete cyber risk mitigation strategy, which includes understanding each organisation's unique cyber risk profile, maintaining organisation-wide cybersecurity awareness, identifying critical assets and developing and testing a business continuity and incident response plan. There is room for improvement in this area however. Less than half of G20 organisations we surveyed reported to manage cyber attacks proactively, and only 10% believe they have no cybersecurity gaps at all.

Shifting to a proactive mindset when attempting to mitigate cyber risk and become resilient can begin with an organisation's first line of defence – their people. Our research shows that 28% of G20 organisations believe 'employee awareness, security, culture and training' are their biggest security gaps, and 35% have invested in this area over the past 12 months. People can be the weakest link in the security chain, or organisations can invest in their own staff and turn them into their strongest asset.

20%

OF COMPANIES WERE VICTIMS OF A RANSOM OR DATA HOSTAGE SITUATION IN 2019

Beyond creating a "culture of security," organisations must proactively assess their digital ecosystem to determine additional vulnerabilities. Malicious actors often look for weak spots as access points and they can leverage connected third parties to gain entry to their primary target. Despite vendors serving as an entry point for hackers, only 35% of those surveyed reported to screen suppliers/clients/other parties, versus 42% in 2019. Cyber resilience involves the protection of internal assets, in addition to identifying and closing any gaps that connected external parties present.

Building a resilient organisation also requires proactive coordination from multiple departments, including senior leadership, instead of leaving cybersecurity to the IT department to handle independently. This holistic approach allows for cybersecurity to be considered as part of strategic decisions, instilling it from the outset versus attempting to address it later. Our research shows that at least half of G20 organisations heavily involve their Board of Directors, Operations, C-Suite, Strategy, or General Counsel/ Legal/Compliance departments in proactive cybersecurity planning. While there is increased recognition by senior leaders that cybersecurity is a business-critical risk, there is room for improvement in this area and resilience is unachievable without their input and buy-in.

NEGATIVE IMPACT

Q. What was the negative impact as a direct consequence of these cyber attacks?

2% Other | **27%** There was no negative impact

SECURITY GAPS VS INVESTMENTS

Q1. Which of the following have you invested in over the past 12 months?
Q2. Where do you believe your biggest cybersecurity gaps are? (Please select all that apply)

EXPERTS WITH IMPACT

ABOUT FTI CONSULTING

FTI Consulting is an independent global business advisory firm dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities.

The views expressed in this brochure are those of the author(s) and not necessarily the views of FTI Consulting, Inc., its management, its subsidiaries, its affiliates or its other professionals.

www.fticonsulting.com

©2020 FTI Consulting, Inc. All rights reserved.