Summary Insights: IT's Biggest Risks and Challenges for 2022

RFG Perspective: IT executives should expect to see increased board-level scrutiny and pressures in 2022 as they cope with the business impacts of an emerging tsunami of IT risks, including cyberattacks and ransomware. We expect that 40 percent of boards of directors will adopt dedicated cybersecurity measures by 2025, which is why enterprises should increase scrutiny for pending mergers and acquisitions – and for supplier/business partner relationships.

Business executives will realize that their corporations must cope with evolving privacy laws, and that they will need to apply high-tech cybersecurity tools and cloud services that can effectively detect, prevent, and remediate consistently across cloud and on-premises environments. Among these will be: security adoption for IoT and OT environments; security enhancements focusing on work from home (WFH); open-source usage and SaaS cloud services. Enhancements must be made to achieve risk mitigation, to meet privacy requirements, and to accommodate remote workforces and increasingly distributed and disparate systems.

Moreover, ransomware incidents and attack vectors are escalating in terms of their disruption and their frequency, even if they remain hidden within corporate IT systems for extended periods of time. This means that IT executives must adopt resiliency and data-integrity postures that will require significant organizational changes. They must evolve the enterprise architecture and infrastructure so that systems will become capable of embedding security controls and maintaining chains of custody for corporate data – no matter where that data resides.

Given the scope of the challenges ahead, IT executives will need to work with the C-suite business executives and with their companys' boards of directors to mitigate risk postures across applications, tools, partnerships, and supply chains. Risk prioritization will be required throughout this process, because corporations will not have enough time or money to achieve all of these security objectives simultaneously.

Cybersecurity and ransomware will once again be top-of-the-list for IT risks in 2022. This will be true, even though IT executives' biggest challenges this year are budgeting and cost containment, strategic planning, and staffing and skills. While none of these items are new, hacker sophistication is increasing – and the technology that will be required to support higher levels of end-to-end security is becoming more complex over time.

46 Kent Hills Lane, Wilton, CT. 06897; (203) 429 8951;
http://www.rfgonline.com/; *Contact: inquiry@rfgonline.com*

On Dec. 8, 2021, the Robert Frances Group facilitated an RFG 100 videoconference entitled: **"IT's Biggest Risks and Challenges for 2022."** This videoconference delineated what the participants believed to be the biggest risks and challenges that IT executives at large enterprises will need to address in 2022.

The panelists for this video conference were:

- Stan Lowe, former CISO of zScaler
- Ev Kontsevoy, CEO, Teleport
- Keyaan Williams, Managing Director, Cyber Leadership & Strategy Solutions
- Anil Karmel, CEO of RegScale
- Malcolm Harkins, Chief Security and Trust Officer of Epiphany Systems

Poll

A quick poll of the attendees on this topic yielded the following results:

- The top two risks that were identified by the conference participants were cybersecurity (44%) and ransomware (44%).
- The next grouping, identified by a third of the respondents were: IAM (identity and access management), vendor risk management, and work-from- home/work-from anywhere (WFH/WFA) environments.
- Perceived to have the least risk by the respondents were Business Continuity/Disaster Recovery (BC/DR), Cloud or Edge security/compliance, data loss protection (DLP) and integrity, and continuous compliance.
- The top three challenges, identified by 56% of the respondents, were DevSecOps, strategic planning and budgeting/costs. Another 44% said that staffing/skills and technical debt were their biggest issues.
- Data architecture and operations management were chosen by 22% of the respondents, while agility/interoperability was mentioned by 11% of the respondents.

Are IT Risks IT Risks?

Panelists hammered home the point that IT risks are not really IT risks at all, but rather are business problems that need to be addressed. As such, the risks fall into three categories: business risks, operations risk (not IT operations but business operations), and technology risk.

46 Kent Hills Lane, Wilton, CT. 06897; (203) 429 8951;
http://www.rfgonline.com/; *Contact: inquiry@rfgonline.com*

In 2022, IT executives need to re-think how they think about risk – and they will have to look at it from a business perspective and work with corporate and line-of-business (LOB) executives on how the issue of risk should be approached and tackled.

IT executives should be thinking about risk not as a geographic problem, but as an overarching threat, for which the architectural complexity is increasing continually. Each new generation of software adds new layers and complexity – as does the addition of new, more complex firmware, hardware, and systems. This increasing complexity elevates the need to use better talent and skills. However, executives must face the reality of pandemic-era staff turnover, which is rapidly becoming endemic, as yet another management challenge.

Strategic Planning

Business executives develop five-year plans every year, while IT executives typically plan for time horizons of one-, three or five-year periods – reflecting the pace at which aging hardware is being replaced.

The mismatch in time horizons for budgets and for infrastructure cycles often gives rise to built-in tensions between the IT executive and business-executive communities. These tensions make coping with ongoing budgetary requirements more difficult than, perhaps, they should be. In many cases, IT executives and business executives have trouble getting on the same page about priorities for protecting the corporation from ransomware the cyberattacks.

But the threat of cyberattacks and ransomware remains – and is growing. In Jan. 2021, the World Economic Forum stated that cybersecurity was one of the top five risks for businesses. There were five reasons for continuing concern:

1. More complexity
2. Fragmentation and complex regulations
3. Dependencies on third parties
4. Lack of cyber expertise
5. Difficulty in tracking cyber criminals

46 Kent Hills Lane, Wilton, CT. 06897; (203) 429 8951;
http://www.rfgonline.com/; Contact: inquiry@rfgonline.com

While there are technical components to this risk, fighting it remains a business problem for the entire corporation – and IT executives will need to focus on and address the business issues first, as they make the case for increased budgets.

The Big Risk Misperception

Business and IT executives do not fully appreciate the extent of various IT risks. For example, many Financial Services firms think that fraud is their biggest risk. Yet, a firmware failure event could prove to be a fatal risk for the corporation, its reputation, and its brand. One example: an instance in which a hacker irreparably destroys the firmware, requiring a full hardware replacement. Such a failure could prevent the firm from returning to normal operations for an extended time – and possibly force the company to permanently close its operations.

Therefore, business and IT executives need to continually contemplate all of the types of risks facing them -- and to understand those risks in context of the business. Then they need to determine what controls and mitigation are required to address those risks.

An often-overlooked area of concern for ransomware and cyberattacks is the vulnerability of senior executives' homes. It may be easier for hackers to pursue, block, and/or blackmail an executive or his family by directing the attack to a residence rather than to a well-defended office or workplace. Periods of global travel also present opportunities for cyberattacks.

That's why IT executives need to be prepared to provide alternative PCs, laptops and/or smartphones for overseas travel, especially in high-risk countries. Alternatively, a complete forensic review of the devices used during periods of travel should be done upon return before they are connected to the network again. Forensic evaluations of the devices are a valuable tool for information-gathering – and for protection against future attacks.

If there is any pushback on the costs of protecting such devices, used during executive travel, IT executives at large enterprises should remind the objectors that the company is already spending millions for physical protection of the executives' sites as well as for the travel protection details. This makes the added IT costs of

protecting executives' PCs, laptops and phones reasonable – and just a bump in the overall protection budget.

Other Considerations

It is IT's job to create trust in the use of organization's digital environment. There are three challenges to be addressed when trying to ensure a safe environment:

- Interoperability – we now live in an API economy. Thus, APIs need to be secured, regardless of who created them or where created.

- Manageability – today an organization's ecosystem is in the cloud, data centers, and at the edge. All of these must be protected. And this especially applies to SaaS governance as well.

- Agility – as companies move at the speed of business, there needs to be transparency and the ability to catch risk exposures as quickly as possible. A "shift left" of security/compliance to the design and code development phases improves the overall enterprise security posture.

One more approach to reducing security risks is running "red teams" that try to find vulnerabilities in the existing IT systems. These exercises are simulations and quarterly tabletop exercises that demonstrate the organization's preparedness for identification, communication, reaction, and remediation of cyber events. Taking the time, effort and funding to run these exercises will help to minimize enterprise risks before they can damage, or swamp, a company's ongoing operations.

Summary

IT executives need to be prepared to deal with cyber risk failures, even if their business executive counterparts have agreed to accept it. Breaches are almost a certainty to occur, so IT needs to have executed a defense-in-depth plan. Moreover, when things go south and someone's neck is on the line, some business executives have been known to attempt to deny or renege on their agreement to certain

exposures and will leave the IT executive to swing in the wind. Thus, having a plan B in place is worth the expense.

RFG POV: 2022 will continue to see an uptick in cyberwarfare attacks from state actors and other malicious groups. The clear intent of these cyber-attacks will be to prevent an enterprise from doing business, with the possible goal of crippling the company so that it is forced out of business. Breaches will almost certainly occur, which is why IT organizations need to have a defense-in-depth plan.

Andy Grove, former CEO of Intel Corp., titled his 1999 management book, "Only the Paranoid Survive: How to Exploit the Crisis Points that Challenge Every Company." In 1999, there was good reason to do so – to prevent crises from up-ending a company's strategy. Now, IT executives must also be paranoid about cyber-risks so that they can protect their corporation's operations, reputation and brand. To do so, they must convince business executives – including senior management and LOB executives, to fund the needed technology and protections.

To achieve that objective, IT executives need to demonstrate the impacts of various cyberattacks in context of the actual business processes (as expressed in business terms). If IT executives make a clear business case to thwart cyber-attacks, then they will be able to gain the funding to construct and support a defense-in-depth posture.

Additional relevant research and consulting services are available. Interested readers should contact Client Services to arrange further discussion or interview with Mr. Cal Braunstein, CEO and Executive Director of Research.

---

46 Kent Hills Lane, Wilton, CT. 06897; (203) 429 8951;
http://www.rfgonline.com/; Contact: inquiry@rfgonline.com