Summary Insights: Making Security First a Prime Directive

RFG Perspective: Enterprises need to drive "security first" best practices that effectively make it a prime directive similar to the "cloud first" directive. Enterprises no longer exist in a world where the corporation contains its proprietary and confidential assets within the confines of its four-walled data centers and colocation sites. The modern world is comprised of a new, more expansive and invasive cloud-enabled reality that is impacting and interwoven with every phase of software development and operations.

Up until now, many business units and IT groups have ignored the business implications and operated in a "business as usual" mode; however, customer lawsuits and legislative scrutiny are changing that at a rapid pace.

IT organizations must begin to clean up their acts immediately or else face significant detrimental, perhaps irrecoverable, impacts to revenue, profitability, reputation, and legal standing. Cultural changes, executive buy-in, and acceptance of security accountability by developers and others will be necessary – along, across, and up the software development lifecycle (SDLC) chain. Issues that are related to progressive infrastructure adoptions, including cloud, hybrid-cloud, SaaS, and Edge frameworks, will drive enterprise IT executives to shepherd the development, security, and oversight methodologies that will be needed to accommodate these evolutions.

IT can no longer hide its secrets – stories of malware and ransomware are front-page news almost daily and companies are being sued by their downstream customers for outages. The costs are estimated to be greater than $20 billion dollars per annum and on the rise.

Companies are exposed to increased security vulnerabilities throughout the entire software development life cycle (SDLC) from internal code, APIs, and third party open-source code, as supplied by cloud providers and suppliers and other business partners and vendors.

On July 28, 2021, Robert Frances Group facilitated an RFG 100 videoconference entitled: **"Making Security First a Prime Directive."** This videoconference examined the need for business and IT executives to put security first and to make it a prime directive across the enterprise and its supply chain.

Key Questions for the Security First Discussion

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

To discuss the adoption of a security-first philosophy in organizations, RFG 100 panelists considered the following key questions:

1. Executives understand that software attacks could significantly damage their firm, but the question is: How do they execute a security first plan that would minimize that risk?
2. What directives need to be issued by the executives?
3. What needs to be done to make sure that each of the individuals involved in the SDLC process accepts security first as one of their responsibilities and how do we eliminate or minimize friction between the groups?
4. What steps need to be taken to ensure security is “shifted left” by all units, and how do you deal with exceptions?
5. How do you get the development squad to improve over time vs. a "business as usual" approach to their work?

The panelists for this video conference were:

- Giri Gururaja, VP, MetLife
- Evan Bauer, CEO, OpStack
- Stefan Liesche, Distinguished Engineer, IBM
- Kimberly Lancaster, Privacy, GRC, and Security Professional

Poll Results

The video conference participants were polled on their organization’s security programs. We found the following results in the polling data for the group:

- 64 percent of the respondents said they execute a security-by-design process that also includes compliance and privacy. In this group, 57 percent stated it was an enterprise-wide process, while 21 percent said they had business unit processes. Only 7 percent of respondents that they had no security by design methodology.
- 43% of the respondents stated it included a “shift left” philosophy.
- Included in the security by design components were the following elements and the percentage that are using those elements:
    - Developer training/education 64%
    - Individual performance plans and incentives 21%
    - Team performance plans and incentives 21%
    - Metrics 50%

- Process improvement goals and measures 50%
- Communications plan and ongoing outreach 64%
- New/revised processes and tools 79%

Business Side Takeaways

A security-first prime directive must start at the top. The Board of Director's risk committee must feel and communicate to the lines of business that security is an existential threat. If that is not conveyed and the commitments obtained by the LoB, then it is highly likely that the initiative will not succeed. All business managers must feel responsible for security to get results. If the directive is to be effective, then the metrics must be results-based, not process-based. Additionally, security must be tied to annual compensation – and it must be part of the executives' performance plan. It should not be considered to be an invitation to hunt for added funding within the corporate budget.

One of the panelists said they felt that the best way to engage executives is to scare them by showing the number of open vulnerabilities, tagged by severity, and tagged by operating system pipeline. The cultural environment must change – and this is one way to instill the desire to change. Executives need to examine the security risks in four ways: financial, legal, operational, and reputational (brand). Then they need to consider process revisions that address all aspects of the security issues and create compensating controls.

Existential threat requires an entire enterprise approach, including the following:

- Create sense of urgency and strategy
- Leadership setting the tone
- BISO/CSO in Business Units take a whole-company approach
- Business Unit accountability
- Building response for cyberattacks into the fabric of the company
- Follow through – e.g., Deming wheel of plan-do-check-act (frequently missing and a major flaw)
- Development and phishing should be a shared understanding between the lines of business and IT, resulting in appropriate policies
- Eliminating the adversarial relationship between developers and security gatekeepers
- Knowing your baseline, risk exposure, and the number of open vulnerabilities and applications that are impacted by them

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

IT and Development Takeaways

As a starting point, business managers need to know the set of all IT assets – i.e., the inventory of systems, including transparency around who owns and who is responsible for each asset and its risk rank. One of the biggest challenges with this approach was thought to be a legacy code problem. That's because many of these assets are undocumented or poorly documented and maintained – and the original developer of the code is long gone, through reassignment, retirement, or death.

It is not all about applications. Data, especially PII data, is everywhere and must be kept secure. One concept is data sparsity, which leads to data sprawl avoidance and reduces the data risk. GDPR (as developed in EMEA) and new mandates, which keep coming from regulatory agencies and governments around the world, are redefining what it means to protect data privacy and to keep the data secure wherever it may be. To do this, there needs to be a change to security engineering practices, as they are described and implemented across the world.

Throughout the IT development and operational chain, people must feel "paranoid". This means that a mindset that questions and examines all potential security flaws is favored in today's business environment. During the event discussion, it was suggested that enterprises utilize a centralized Security and Privacy By Design (SPBD) policy and implement SPBD processes in each of the development and operational units. That is, the policy would be controlled centrally, while each of the different teams can implement the policies with different methodologies, regardless of the tool sets and languages being used.

Enterprises need to create common measures and incentives and commit to education on security for all users and managers. However, the entire development team doesn't have to use all same tools. Rather, it will be necessary to automate the CI/CD processes and establish meaningful security controls. Initially, it will be necessary to have an automation process that has exception-based processing allowances. That approach is a proven one – and it should be carried into the future.

IT executives need to think about the entire process, and they also need to measure the developers overall. Executives should score how well developers did on training courses, as well as knowing the percentage that completed the training courses. It is also important to measure developers' code quality improvement – not just the quality of individual applications. IT should measure the rate of code fix and exposure level – that is, finding out how quickly bugs are closed out and finding out the number of remaining open critical and high vulnerabilities. If possible, companies should do threat modeling by developer. If there is at least one good

developer rock star, he/she should train others, especially the bad ones. They should be doing code reviews and paired coding exercises.

One of the panelists suggested a three-in-a-box development and squad structure for the infrastructure. Here, a practice leader (hopefully a rock star) should be the owner/squad leader. Each squad expert should share a range of customer success stories and solutions, and then recommend changes for process, tools and policies. The objective here is to shift security "left."

Another panelist suggested creating security champions in development (co-created with development and security), along with the following elements:

- Community challenge (not just individual)
- Champions should be viewed as evangelists with a career path
- Tools and training/upscaling
- Code scanning
- Rewrite standards – security and privacy by design [SPBD]
- Training mandates
- Hackathons – with competition amongst groups
- Incentives and gamification and recognition (leader boards)
- Team competition

Another concept was the building of a factory model for third-party remediation for legacy applications. In many cases this will be offloaded to outsourced services providers. If this happens, to ensure successful outcomes, the offshore firms providing these services should be held accountable to their contract commitments. This approach is also true for all shadow IT – especially for assets on Internet sites and orphaned sites. All these components of the overall software landscape should be included as part of the enterprise's asset inventory.

Summary

Most organizations are a long way from having "security-first" as a prime directive. Enterprise and IT executives need to change the corporate culture – and making it a culture in which all employees must consider privacy and security to be part of their daily routine. Annual performance and code of conduct reviews alone will not make this happen.

Rather, this sweeping change in corporate culture will require a major ongoing commitment from the top management. Otherwise, all levels of management and staff will not be positioned to implement effective security safeguards as an integral part of their work ethic, day in and day out.

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

RFG POV: Most Boards of Directors and senior corporate executives do not treat security as a prime directive. They are willing to compromise on security risks without fully understanding the extent to which the enterprise is exposed by these risks. To effectively deal with risk exposures, IT executives must understand, evaluate, measure, translate, and communicate the risk exposures and obtain the resources needed to address the ones that could be materially significant or existential threats to the business. IT executives should also adopt processes – from training to operations – that will continuously improve their privacy and security risk exposures. This approach to security will drive their teams to continuously improve their privacy and their security track record.

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*