Infosys®
Navigate your next

VIEWPOINT

# SECURITY BY DESIGN

Good security wins customers, empowers employees and streamlines compliance. However, most organizations continue to view security as just a technology issue. Instead, CXOs must work with business and technology leaders to design security into systems, processes and people from the start. To get there, companies must remember that their enterprise is just one node in a larger network.

Infosys® | Knowledge Institute

Global spending on cybersecurity products and services will exceed $1 trillion cumulatively over the period from 2017 to 2021.[1] It will account for 10% of overall IT spending in 2020.[2]

> Secure by design reduces overall cybersecurity risk and cost of ownership while improving customer confidence

Even so, most companies incorporate security into systems just before deployment in a bid to meet compliance and internal security assessment criteria. More proactive firms integrate security into their systems from the very beginning. However, even these firms fail to ensure that their workforce understands security protocols, and they lack effective governance processes to put security controls in place. As the threat landscape increases due to massive digitization across industries and the integration of "internet of things" and operational technology with IT, this 'people and process' element is now more important than ever.

Done effectively, this more holistic "secure by design" approach will reduce the overall cybersecurity risk from internal and external threats. Properly devised, it can also reduce costs and aid the organization in increasing customer satisfaction from enhanced customer confidence.

## A widening threat landscape with fewer security experts

As major firms strive to keep pace with their young, mobile and connected workers, some experts say that it has become easier to hack into an organization, steal its secrets or create havoc with its data systems. Employees can now work on their own portable devices, including smartphones, tablets and laptops. This "bring your own device" movement is accelerating the development of a market that is projected to hit $367 billion by 2022, up from $30 billion six years ago.[3] Such devices increase the exposure to malicious applications and viruses, and disclose precious intellectual property if the device is stolen. Hackers are also known to create trust through the use of popular applications and subtly request sensitive information. Eighty-five percent of mobile apps have little to no protection, which allows criminals to continually harvest data, connections and resources from the wider business ecosystem.[4]

The fact that large organizations are often just a node in a wider network further increases cyber risk. Hackers often target weak links in partner organizations. Many breaches occur when lax security by third-party vendors exposes system credentials, which can be used to install malware that captures credit card or other sensitive information. With the advent of the cloud, internet of things and operational technology, businesses are more connected than ever to a wider network of partners, sharing ever more data without full assurance that proper security measures are in place.

Open-source software is also a problem. Business software now comprises more than 50% of open source code.[5] Firms may be using outdated open-source libraries that are easy for hackers to penetrate. In fact, research shows that 78% of audited codebases contain at least one open-source vulnerability, of which 54% are very high risk.[6]

This would all be manageable if firms had the talent to instil security into systems and processes from the start. However, security experts are in short supply. One estimate predicts there will be a shortfall of 1.8 million security workers by 2022.[7] Seven in 10 software developers are expected to write secure code, but less than half receive adequate training.[8]

> 78% of audited codebases contain at least one open-source vulnerability, 54% of which are very high risk

To fight back, firms must make security part of their DNA. They must upskill employees, build secure software development pipelines and implement effective security controls across all people, processes and technologies.

# Security by design

Security mechanisms such as threat intelligence platforms and penetration testing do much to thwart attackers and expose system vulnerabilities. Good software can be designed by weaving in security, compliance and privacy requirements into the requirements documents. Security is then embedded during the architecture and design phases so that code can be released speedily with increased confidence.

Organizations must also ensure that sensitive information is masked when moved to non-production environments that may not have sufficient security controls in place.

However, beyond securing the systems themselves, firms can do six things to ensure appropriate governance is in place and that people don't become the weakest link in the chain.

## Six things all firms must do

These days, many businesses don't just invent new code; many create devices, products, even platforms based on that code. Anytime anyone in the organization creates anything, they must first come up with a security architecture review process for all the systems that they develop or procure from third parties. This review covers security considerations in the architecture, such as authentication and authorization encryption approaches. Senior management, as high up as board level, have to highlight why it's important for every company unit to adhere to this process.

Second, threat modeling should be carried out for very complex projects. This process involves looking at code from the perspective of a potential hacker and identifies threats in advance. The STRIDE framework, which was first implemented by Microsoft to identify system entities, possible events and the boundaries of the system, can be used here. This helps in designing code that is safe from identity spoofing, data tampering, information disclosure, denial of service (exhausting the resources needed to provide a service) and allowing someone to do something they are not allowed to do.[9]

Third, every person in the company ecosystem, whether employee, vendor or partner, should undergo security awareness training. This "second line of defense" education should be easy to understand and based on business terms. Negligence of security protocols is often more of a threat than malicious behavior. Firms can segment their teams based on the groups at risk of fraud or exposure and educate them on proper cyber procedures.

Fourth, organizations must have a governance process in place for usage of open source software. Only security tested and legally vetted open source components should be used by development teams.

Fifth, DevSecOps, a security-led variant of the DevOps method of software development, can be used to design secure code faster and more cheaply. Here, security practices, standards and tools automate the software development life cycle by fusing business, development, testing, infrastructure deployment and operations. This reduces the time spent in scans and ensures compliance with ever-stricter regulations. To aid in this, experts can be brought in to the DevSecOps process to train small teams in secure agile development. They must be innovative thinkers, quick on their feet and open minded. With this operating model in place, security is naturally seen as an integral and critical part of a well-oiled machine.

Finally, and most importantly, the C-suite must be involved in the effort, and time must be invested in developing a clear vision for what "secure by design" means within the firm. The function of the chief information security officer should

be empowered, and the officer must report to the board. Assets must be rated on their level of importance, and more investment must be plowed into systems that are more complex or risky.

## The extended ecosystem

Security by design must extend beyond the gates of the enterprise. It is of great importance to remember that most large corporations act as a node in a much larger network of suppliers, partners, distributors and regulators. It is critical then that all third parties are safe to bring on board.

Firms must confirm internal systems are secure by design while making sure security is embedded into contracts when third parties are on-boarded. Guidelines must be in place to ensure third-party relations are safe. Third-party risk management can be used to do due diligence and determine the suitability of a vendor for a given task and whether they can keep information secure. Good processes include review, monitoring and management communication over the entire vendor life cycle.

"It takes 20 years to build a reputation and five minutes to ruin it," said Warren Buffet. To ensure those five minutes aren't due to breaches in insecure systems or employee negligence, business leaders must quickly learn to speak the same language as their security counterparts. Once sponsorship comes from the very top, employees will be invigorated to ensure that systems are secure and will be more vigilant about how and where they use devices out of office. Partners will trust that their data is being carefully safeguarded beyond corporate perimeters. Customers, for their part, will be more loyal, resting safe in the knowledge that their data is secure. And businesses will view security not as a necessity but as a differentiator for gaining share of wallet.

## References

1. Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021, Cybercrime Magazine
2. Businesses Use AI to Thwart Hackers, WSJ Pro Cybersecurity
3. The Future of BYOD: Statistics, Predictions and Best Practices To Prep For The Future, Forbes
4. Cybersecurity Trends in 2020: BYOD and Mobile, Technology Advice
5. How GitHub secures open source software, GitHub
6. 5 Open Source Security Risks You Should Know About, xfive
7. Confronting the Cyber Talent Crunch in Consumer Products, WSJ
8. Software Developers Face Secure Coding Challenges, Dark Reading
9. Threat Modeling: 12 Available Methods, Carnegie Mellon University

## Authors

**Sujatha Mudulodu**

*Cyber Security Practice Manager – Infosys*
MSujatha@infosys.com

**Harry Keir Hughes**

*Senior Consultant – Infosys Knowledge Institute*
Harrykeir.Hughes@infosys.com

## About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.

To view our research, visit Infosys Knowledge Institute at infosys.com/IKI

Infosys®
Navigate your next

For more information, contact askus@infosys.com