CISO Q&A: HOW TO AVOID THE UNINTENDED RISKS OF DIGITAL TRANSFORMATION

Rohit Ghai, president at RSA Security, asks compelling questions that are designed to head off potentially disastrous consequences at the world's largest organizations. For instance, a couple of years ago, he asked, "Is the cyberworld doomed to be unsafe forever?"

Now Ghai has the full weight of his entire company around a bold question they've aimed at C-suite executives, chief information security officers (CISOs), IT and security leaders globally—What is digital risk?

RSA explains that digital risk refers to the new and often unexpected consequences of digital transformation, and it's becoming a top concern for business and IT executives.

"Digital transformation is not something new. It is true about everything we have done in the past and everything we are going to do in the future," says Zulfikar Ramzan, Ph.D., chief technology officer (CTO) at RSA Security. "To be successful, we have to engender trust in new technologies, and managing digital risk is about fostering that trust. The more trustworthy people believe technologies are, the more likely they will take that leap of faith to embrace and adopt them."

In an interview with Cybercrime Magazine at RSA Conference USA 2019 in San Francisco earlier this year, Ghai took it a step further when he said that digital risk management is a broader concept than cybersecurity.

Ghai calls digital risk both a boardroom topic and a team sport that requires IT and the security office to work together with business stakeholders.

After hearing the definition of digital risk, Cybercrime Magazine decided to formulate some follow-up questions—with the help of RSA Security—for large enterprise chief risk officers (CROs) and CISOs to answer.

The following security leaders agreed to go Q&A with our editors:

- Deneen DeFiore is SVP, global chief information and product security officer at GE Aviation. During her 18-plus years with GE, she's held numerous senior technology management roles at GE Corporate, GE Energy Services and GE Aviation. DeFiore is a board member for the Aviation Information Sharing and Analysis Center (A-ISAC).
- Paul Caulfield is the CRO at Israel Discount Bank (IDB), a global financial services company with offices throughout the U.S., in Israel, and in Latin America. He was previously head of compliance at U.S. Citi Commercial Bank. Caulfield is also a former assistant district attorney at the New York County District Attorney's Office.
- Dr. Jay is the CISO for Xerox and a former White House deputy CIO. She was previously the first CISO at Stryker. Dr. Jay spent more than 11 years as an adjunct faculty member for several well-respected universities, and six years as a cryptologic engineer at the U.S. Department of Defense (DOD).

This is the first of a four-part series from Cybercrime Magazine, sponsored by RSA Security. In each one, we'll hear from three large enterprise senior security leaders. We posit the most likely way for organizations to avoid the unintended risks of digital transformation is to learn from each other.

ORGANIZATIONS ARE PURSUING DIGITAL TRANSFORMATION TO REMAIN COMPETITIVE IN THE MARKET. DO YOU THINK THERE ARE UNINTENDED CONSEQUENCES OF ADOPTING NEW TECHNOLOGY?

Paul Caulfield: “Inherently (the most important word here), unintended consequences are always lurking.”

Deneen DeFiore: “Yes, in a digital business model, we are moving to a framework that gives each person in our organization increasing autonomy in how he/she uses information and devices—and what level of security they adopt. That also comes with recognition and understanding that those decisions may have consequences and impact. We need to start ramping up education and awareness and give people the knowledge to make the right decisions.”

WHAT WOULD YOU SAY ARE SOME OF THOSE UNINTENDED CONSEQUENCES MORE SPECIFICALLY?

Paul Caulfield: “Failure of effective challenge that could have mitigated, for example, an incomplete inventory of what personal information is captured, why each piece is captured and what would lead to this information no longer being needed to then discard it safely.”

Deneen DeFiore: “One specific example is the use of consumer-type messaging apps to manage business transactions and communications. While it’s easy and low cost, many companies do not have a contractual relationship with the app providers and can’t ensure security controls to protect their company’s information. In many cases, regulators’ expectations are that a company has a duty to preserve data when business is performed over these messaging apps. Most employees aren’t aware their actions may be putting the company at risk.”

IN THE INDUSTRY IN WHICH YOU WORK, WHAT ARE SOME OF THE WAYS ORGANIZATIONS ARE INNOVATING?

Paul Caulfield: “Sadly, catching up to fintech firms. Happily, given the resources financial institutions have, they’re covering that ground up in increasing speed, by either partnering or acquiring the fintech or developing or partnering with other FIs to create new ways in which to share information, make decisions or trade.”

Deneen DeFiore: “In the aviation industry, operating the best engines, components and systems can be improved using data and analytics. A generation ago, a GE Aviation engineer would have been on the cutting edge of technology using small sets of data gathered after each flight to enhance the performance of our equipment in service. This was the limitation of the technology at the time, but today, digital connectivity is removing that barrier.”

Dr. Jay: “Organizations are using predictive and behavioral analytics as well as AI to assist with fighting spear phishing. As technologists we’ve talked about using AI in technology but taking it deeper into cybersecurity—which drives innovation further.”

WHAT ARE SOME OF THE TECHNOLOGIES THEY’RE ADOPTING?

Paul Caulfield: “I’ll give two examples—information sharing in secure channels to identify, report and mitigate money laundering and fraud and blockchain to accomplish core functions such as trading and identifying customers (i.e., KYC).”

Deneen DeFiore: “We are applying data analytics and new digital technologies to advance our own operations. Digital design tools based on additive manufacturing, advanced automated machining and inspection, all are enabling our operations, dramatically reducing cycle time while improving quality. For example, our most sophisticated turbine blade design concepts are now on test in two weeks, not the nine months it once required, thanks to rapid prototyping and 3D printing.”

Dr. Jay: “Robotic process automation (bots) has always been used in a malicious way within cybersecurity but now I see the usage changing to help us thwart the adversary. Also consider that machine learning has been discussed a lot with technology but is now being extended to help identify spear-phishing emails.”

HOW BIG OF A CHALLENGE DO YOU THINK THESE NEW DIGITAL RISKS ARE FOR BUSINESSES?

Paul Caulfield: "Big. Huge. The lack of integrity of data within existing, usually antiquated and even decentralized systems is the basis of 'garbage in/garbage out.' The speed to market and intensity of competition exacerbate this risk—businesses will implement really neat tools that will fail entirely because no one will have confidence in the outputs. Most frighteningly, they won't know that and make a critical decision based on incorrect data."

Deneen DeFiore: "It's a big challenge for companies today. In today's digitally enabled business model—for example, in GE's case, where our customers are relying on us to manage high-value assets like jet engines for optimal performance—a data breach or service outage breaks trust. The customer won't be mad at the firewall that failed, or the admin that misconfigured a cloud VPC. They lose trust in GE. So, protecting our customer relationships means managing cybersecurity and technology risks."

Dr. Jay: "The challenge is extremely huge. The digital landscape is based on connected infrastructures. The digital risks are highly based on data. That risk is not just centered around the availability of that data but highly dependent upon the integrity of that data."

DO YOU THINK ORGANIZATIONS ARE ADEQUATELY PREPARED TO MANAGE THOSE DIGITAL RISKS?

Paul Caulfield: "They are getting better because they're becoming more aware. That's one reason why some AI and blockchain solutions remain in early stages."

Deneen DeFiore: "I think we are getting there. There isn't a known blueprint, but the conversations are happening, and that is progress. There is a general awareness and understanding that managing cybersecurity, privacy and data protection risks is key to the success of any digital transformation."

Dr. Jay: "Are you ever truly prepared? We have to have solid risk frameworks. Those frameworks have to continuously evolve in relation to the company's risk appetite and the threats. Our risk scores have to be meaningful to the business and showing how the risk affects profit, growth and revenue."

HOW DO YOU THINK SECURITY AND RISK TEAMS COULD BE WORKING TOGETHER TO ADDRESS THIS CHALLENGE?

Paul Caulfield: "Sharing information more courageously and collaborating for the greater good, not the almighty dollar."

Deneen DeFiore: "You must operationalize the way you manage risk cross-functionally and holistically across the entire business. Cybersecurity risk management is a business function. It's not just a technical problem. So, our responsibility as cybersecurity and risk professionals is to ensure cyber risk is known, evaluated and incorporated into business decisions (e.g., business development opportunities, supplier, third-party agreements, customer agreements, etc.) from ideation and innovation, design, build and launch, to support, service and operations."

IS YOUR ORGANIZATION LOOKING FOR NEW WAYS TO ADDRESS AND MANAGE RISK?

Paul Caulfield: "Always, starting with empowering and educating our people."

Deneen DeFiore: "Yes, we are. We are incorporating cybersecurity risk management into our business-wide Enterprise Risk Management framework. We are trying to characterize and quantify cybersecurity risks in a consistent manner to other ERM risks and drive shared accountability. We are also relying more on data analytics and leading risk indicators to make the best risk treatment decisions."

Asking questions does not remove the digital risk that organizations are faced with today, but it's a step in the right direction. Ghai and RSA are pushing the envelope with questions more so than with anything else. And the CISOs are clearly responding.

DIGITAL RISK IS EVERYONE'S BUSINESS
HELPING YOU MANAGE IT IS OURS

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change.

Find out how to thrive in a dynamic, high-risk digital world at rsa.com.

This article originally appeared in Cybersecurity Ventures. "CISO Q&A: How To Avoid The Unintended Risks Of Digital Transformation," May 10, 2019. Sponsored by RSA. Reprinted with permission.

RSA