Cyber Resilience: Navigating an Evolving Risk Landscape

FEATURED EXPERTS

Austin Berglas, Global Head of Professional Services at BlueVoyant

Geoff Brown, Chief Information Security Officer and Head of New York City Cyber Command, City of New York

Tim Murphy, Chairman of the Board, Thomson Reuters Special Services, Thomson Reuters; CEO and President, Consortium Networks

Lauren Dana Rosenblatt, Executive Director, Deputy Chief Information Security Officer (CISO), The Estée Lauder Companies

Kevin Zerrusen, Former Managing Director and Head of Technology Division Risk Governance, Goldman Sachs

MODERATOR

David Lawrence, Founder and Chief Collaborative Officer at RANE

Cybersecurity risks are ever-evolving and posing threats to increasingly large numbers of businesses, communities, and even governments. Yet, many of the crimes that exploit cyber vulnerabilities are crimes societies have been dealing with forever: theft, extortion, and corruption. RANE gathered a group of cybersecurity experts to discuss why these age-old crimes are so confounding in the digital age.

The main reason there has been no concerted government or business response, cyber roundtable participants agreed, is that there has been no "inflection point," no single instance that has captured the government's, the business community's, and the public's attention to focus around cybersecurity.

- Though there are cyberattacks and security breaches every day, the general public does not seem to be concerned by them or does not fully understand how they are impacted in their day-to-day lives, **Brown** said.

- Instead, most people view cyberattacks as something that "just happen," said **Rosenblatt.** Cyberattacks resonate like the power going down, she said: "Oh, the power went down, but it will come back. Oh, there was a cyberattack, but they will fix it."

- **Further, cyberattacks and breaches have become so ubiquitous, panelists said, that people and companies may simply be expecting them to occur and working them into their baseline risk analyses**

- Specifically on the business front, some companies have proven remarkably resilient to cyber threats, **Rosenblatt** said. **Berglas** agreed, saying that most companies simply want to get back up and running after a cyberattack and are not concerned with influencing a national narrative around the vulnerabilities.

A key component of the continued lack of key regulations around cybersecurity, said Zerrusen, is that the major actors are still exploring the new capabilities that cyber vulnerabilities create. Contributing to this "uncharted territory" are disagreements over basic definitions. Whether an action is a cyberattack or corporate espionage, for example, is still debated, as is whether a distinction between the two is needed or important.

- Not all governments and companies, and not all departments within those governments and companies, see cyber vulnerabilities the same way. Some, said **Zerrusen**, see them as opportunities.

- These groups, which hold sway over corporate and government responses and policies, are not ready to give up what they see as a valuable tool in order to address vulnerabilities.

It is not enough to move organizational data to the cloud and assume it is safe; companies should know the specific controls the cloud is employing and check them regularly.

In order for there to be a proper response, Brown said, three things are necessary: public demand for action from both the government and businesses; the capability to respond; and trust that the problem is being addressed. So far, all three have been lacking.

- Russian interference in the 2016 election put all levels of federal and state governments on high alert to the expanded risks of cyber vulnerability, extending the threat from expected hacks to manipulation of online information, said **Murphy.** He lamented, however, that governments "have not caught on in a sufficient manner to respond in an effective, scalable fashion."

- While the federal and state governments are on the forefront of addressing wider cybersecurity issues, said **Zerrusen**, they need to be better at selling the problem to the public as a "wholistic" issue, argued **Murphy**: the government needs to present the threat as one that risks people's money, their jobs, their homes, and their livelihoods.

- **Berglas** said that he is concerned that the inflection point necessary to raise the appropriate level of concern and awareness will never happen due to confusion over the severity and potential impact of certain cyberattacks. He points to Russian interference in the 2016 election as a key example of a cyberattack that should be concerning to all Americans. "We're dealing with issues today that we dealt with 10, 15 years ago," he added, "and we still haven't made enough progress to prevent Russian influence in our democracy."

Many enterprises, meanwhile, are increasingly adopting a "general framework" to respond to cyber security risks, said **Rosenblatt.**

- Companies should see cyber risks as important as financial and reputational risks. The fact the businesses are spending an increasing amount of money on cybersecurity shows that more companies are adopting this outlook.

- Despite the improved outlook, **Zerrusen** predicted that cybersecurity costs will only grow as threat actors and vectors increase.

These frameworks, though, show a distinct weakness of cyber responses, said Brown: Responses have been siloed to different agencies and departments. Both the government and businesses will need to adopt a cross-agency, cross-sector approach to properly respond to cyber threats, he added.

While the proper response is being formulated, there are a number of steps companies can take to better insulate themselves from cybersecurity risks, both Rosenblatt and Zerrusen said.

- **Education is key**. Companies should make an effort to educate all their employees, from C-suite on down, about cybersecurity techniques. Further, they should educate them about techniques they can use in their private lives, and not just ones that can be applied at work.
  Companies should move their data and operations to a secure cloud. However, businesses need to be incredibly knowledgeable about the cloud service they are using. It is not enough to move the data and assume it is safe; companies should know the specific controls the cloud is employing and check them regularly. Further, all IT equipment should regularly be audited and checked for vulnerabilities.

- Customer data, transaction data, and company communications need to be classified and sorted, as well as encrypted. While encryption is becoming the norm, it may be necessary to choose which data and communications are encrypted. If this is the case, a comprehensive audit and data ranking system becomes necessary

- Finally, companies need to understand the risks of "bring your own device" (BYOD) workstyles. More and more companies are relying on employees working on personal devices or giving out devices that are not isolated only to work purposes. This exposes the business to any number of new risks as company data becomes far more accessible.

FURTHER READING

China's Cybersecurity Law: Navigating Security and Compliance

Spyware: A Growing Threat in Today's Cyber Landscape

The Entangled Enterprise: When Personal Cyber Risk Becomes Corporate Risk

RANE Podcast: Improving Cybersecurity for the Private Client

Addressing the Current Gaps in Cyber Staffing

ABOUT THE EXPERTS

Austin Berglas, Global Head of Professional Services at BlueVoyant

Austin Berglas came to BlueVoyant after building and leading the Cyber Defense practice at K2 Intelligence. Prior to K2 Intelligence, he served 22 years in the U.S. Government. Berglas was the Assistant Special Agent in charge of the FBI's New York Office Cyber Branch. There, he oversaw all national security and criminal cyber investigations in the agency's largest cyber branch, and was awarded the FBI Director's Award for Excellence in a Cyber Investigation. Prior to the FBI, Berglas achieved the rank of captain in the U.S. Army.

Geoff Brown, Chief Information Security Officer and Head of New York City Cyber Command, City of New York

Geoff Brown was appointed Chief Information Security Officer for the City of New York in 2016, a position focused on cybersecurity and aggregate information risk across all 100+ NYC departments and agencies. In July 2017, Mayor de Blasio established New York City Cyber Command, led by Brown and charged with setting citywide cybersecurity policies; directing response to cyber incidents; and advising City Hall, agencies and departments on the city's overall cyber defense. Prior to joining city government, Brown worked in financial services, developing and operating threat management disciplines including threat intelligence, detection, response and countermeasures.

Tim Murphy, Chairman of the Board, Thomson Reuters Special Services, Thomson Reuters; CEO and President, Consortium Networks

With 30 years of public and private sector experience — primarily in the Federal Bureau of Investigation — Timothy P. Murphy is a recognized leader in the global law enforcement, intelligence, and business communities. Murphy maintains close ties to the law enforcement and intelligence communities and is frequently consulted for his expertise in global cyber, counterterrorism, intelligence, criminal, and security issues and is a guest lecturer at colleges and universities on these issues. He is frequently called upon to speak on these topics in the media. He is member of the Police Executive Research Forum, the International Association of Chiefs of Police (IACP), the Department of State Overseas Security Advisory Council (OSAC), Deputy Co-Chairman of the FBI/ DHS Domestic Security Alliance Council (DSAC), the FBI Agents Association, and the FBI National Academy Associates. He is also member of the Advisory Board of two cyber-security companies, on the Board of Directors for a data analytics company, and The Foundation Board of Directors for Ferris State University.

Lauren Dana Rosenblatt, Executive Director, Deputy Chief Information Security Officer (CISO), The Estée Lauder Companies

Lauren Dana Rosenblatt is Executive Director, Deputy Chief Information Security Officer (CISO) for The Estée Lauder Companies. Rosenblatt serves on the Retail and Hospitality Information Sharing and Analysis Center (RH-ISAC) Board, National Retail Federation (NRF) IT Security Council Executive Committee (Board) and SINET Innovation Awards Committee. Previously, Rosenblatt was the Global Head of Cyber Threat Management at The Estée Lauder Companies, where she led the Security Operation Center (SOC), including security analysis, threat intelligence, incident

response, vulnerability management, pen testing, mobile security and cybersecurity metrics. Prior, Rosenblatt was the Global Head of Insider Threat and Vendor Risk Management at The Blackstone Group; she also advised cybersecurity startups and guided 70+ CISOs of Blackstone Portfolio Companies. Previously, as a Vice President in Technology Risk at Goldman Sachs, she launched a Firmwide Insider Threat Program, led the Internal/External Cybersecurity Exercise Program, ran multiple cybersecurity senior steering groups and led a cybersecurity and threat intelligence technology integration team.

Kevin Zerrusen, Former Managing Director and Head of Technology Division Risk Governance, Goldman Sachs

Kevin Zerrusen was previously Global Head of the Regulatory and Controls Team and earlier Global Co-Head of the Security Incident Response Team, Goldman Sachs. Prior to joining Goldman Sachs in 2013, he had a career in the Central Intelligence Agency (CIA), where he served in multiple roles at the agency's headquarters in Langley, Virginia and overseas. He most recently directed a cyber center at the Central Intelligence Agency.

David Lawrence, Founder and Chief Collaborative Officer, RANE

David Lawrence previously served for approximately 20 years as Associate General Counsel and Managing Director at Goldman Sachs. During his tenure, Lawrence formed and was the global head of the Business Intelligence Group. His role covered a wide range of legal, regulatory, diligence and transactional responsibilities for the firm, as well as advising Goldman's clients directly. Lawrence served on a number of the firm's global risk-management and investment

To speak with any of the experts mentioned in this recap, please contact RANE for an introduction.

ABOUT RANE

RANE (Risk Assistance Network + Exchange) is an information and advisory services company that connects business leaders to critical risk insights and expertise, enabling risk and security professionals to more efficiently address their most pressing challenges and drive better risk management outcomes. RANE clients receive access to a global network of credentialed risk experts, curated network intelligence, risk news monitoring, in-house analysts and subject matter experts, and collaborative knowledge-sharing events.