June 2nd, 2021

WSJ PRO CYBERSECURITY EXECUTIVE FORUM

TAKEAWAYS FROM THE WSJ PRO CYBERSECURITY EXECUTIVE FORUM

DECEMBER 1ST, 2021

The Road to Recovery

Mr. Ramakrishna said it would have been irresponsible had the company not publicly reported details about the widespread hack SolarWinds discovered last December.

He described the breaches SolarWinds and Microsoft suffered “as the price you pay for ubiquity.” Software deployed in a very large number of organizations with administrator-level privileges presents an attractive target for attackers.

It is still not clear how attackers penetrated the SolarWinds network. Mr. Ramakrishna said, “we boiled it down to three possibilities: a spearphishing attack, a password-spraying attack or a zero-day vulnerability. If you were to ask me without knowing anything what was my first guess, my first guess was a targeted spearphishing attack. But there’s no way to confirm it.”

Mr. Ramakrishna’s advice to small and medium-sized organizations is not to look at security as an afterthought. It should be designed into everything the organization does and should be thought of in terms of quality.

Sudhakar Ramakrishna
President and CEO
SolarWinds

Reinforcing the Supply Chain

Mr. Perullo and Mr. Overly highlighted ways businesses can address cybersecurity protections in their vendor and business partner engagements. The advice included:

- Conduct due diligence through specific security questionnaires and on-site inspection of what the vendor is actually doing. This can help the firm identify issues.

- Carefully craft contract language to ensure specific information protection controls and a clear outline of the vendor's responsibilities, such as timely breach notification and liabilities.

- Consider how external and internal products are deployed and architected to limit their permissions and capabilities only to their purpose.
  This can reduce the adverse impact to the business in the event of malicious activity.

Jerry Perullo
Former CISO
Intercontinental
Exchange

Michael Overly
Partner
Foley & Lardner

Healthcare in the Crosshairs

Ms. Hughes said though 'Internet of Medical Things' technology has been embraced by the healthcare industry during the pandemic and has benefitted medical experts, some devices present a risk. She explained having the appropriate controls and using segmentation to protect against attacks spreading to other devices are important.

Mr. Johnson highlighted hiring talent as a key challenge. He explained: "even if my CFO said 'Hey, here's $50 million, go hire all the people you want,' it's very challenging to get those qualified people." He described the situation as "a very difficult perfect storm" where existing resources are becoming more stressed and the threat level is increasing. "It's hard to resource the problem away," he said.

Ms. Hughes's team uses the National Institute of Standards and Technology Cybersecurity Framework to help secure their network, while Mr. Johnson said not all of his firm's solutions are solved by technology. Premise Health has conducted voluntary training sessions for employees, while reducing the number of dedicated vendors among the company's business partners.

Kathy Hughes
VP and CISO
Northwell Health

Joey Johnson
CISO
Premise Health

WSJ PRO CYBERSECURITY EXECUTIVE FORUM

Reshaping the Government Role

Since the creation of the ransomware task force in June 2021, the Department of Justice has been working with victims to collect information that allows action to be taken against the attackers, including seizing money and dismantling infrastructure, and the ecosystem that enables cybercrime.

Mr. Carlin said incomplete data on how many companies are victims of ransomware and other attacks hinders efforts to determine the full impact of the government actions. “The way that we know about attacks, often, is because of a report from the victims, and right now, not all victims are reporting.” He added that without this information, it was hard to assess the efficacy of the government’s response to rising cybercrime.

Cybercrime is “a serious risk” according to Mr. Carlin, and the best way to protect your company is through resilience, a defense-in-depth approach and having the right team in place so you can prepare for--and practice for--the worst. He added companies should never make a ransomware payment without first telling the government. “You just don’t know who you are paying.”

John Carlin
Principal Associate Deputy Attorney General of the United States

Regulation Around the World

Ms. Wugmeister said Asia has increasingly stringent and comprehensive privacy laws and requirements. These include data localization, limitations on cross-border data transfers, providing privacy rights and faster notification. China, for example, requires firms to report a breach in eight hours if the incident affected the data of more than 100,000 people.

In Europe, the General Data Protection Regulation brought significant security obligations for firms and rights for individuals, said Mr. Azim-Khan. Regulators are looking to enforce new rules under the GDPR “more aggressively” than before, he said. Mr Azim-Khan believes the grace time for companies to understand the concept of Privacy by Design is now over.

The U.S. approach to cyber is complex because it doesn't have a single unified set of cybersecurity rules, resulting in complexity for firms, said Mr. Swaminathan. He advises firms to look at enforcement actions to understand where the trends are. For example, according to Mr. Swaminathan, the Securities and Exchange Commission and the New York Department of Financial Services are the regulators moving the needle on enforcement.

Miriam Wugmeister
Co-Chair, Global Privacy and Data Security Group
Morrison & Foerster

Rafi Azim-Khan
Partner
Pillsbury

Aravind Swaminathan
Partner
Orrick

WSJ PRO CYBERSECURITY
EXECUTIVE FORUM

WSJ Pro Cybersecurity Survey Results

The WSJ Pro Research team presented data collected in a survey of U.S. cybersecurity professionals. Among the key findings:

- Fifty-one percent of companies said they were ‘very unlikely’ or ‘somewhat unlikely’ to pay a ransom, a decline over the 2020 figure.
- A majority of large companies reported that hiring new cyber talent had become more difficult over the past year, although efforts to recruit a more diverse workforce, including women and people of color, have been successful at many businesses.
- Only 5% of small businesses surveyed reported having a CISO in charge of cybersecurity. Forty-four percent reported the chief executive or founder led cybersecurity efforts, which may result on some small companies being exposed to technical risks.
- More than two-thirds of companies said they have cyber insurance policies, an increase from roughly half in 2020.

Download the full report at https://www.wsj.com/pro/cybersecurity/research

Rob Sloan
Research Director
WSJ Pro
The Wall Street Journal

David Breg
Research Director
WSJ Pro
The Wall Street Journal

WSJ PRO CYBERSECURITY
EXECUTIVE FORUM

Scoring Board

Mr. Levi, Mr. Rohrbaugh and Dr. Lauterbach shared their advice for how security executives should approach dealing with boards. This included:

- Understand how your board prefers to consume information and whether formal presentations can be complemented with informal discussions.
- Avoid surprises. The board should only receive information that is available to management.
- Identify the level of cybersecurity awareness and knowledge board members have in advance and adjust your approach accordingly.
- A security strategy should be rooted in the business strategy and show how it will address threats to the organization's value generation.
- Communicate facts and if possible, actionable quantitative metrics. Avoid spreading fear, uncertainty and doubt.
- Talk about where the program is, where it should be, where gaps exist and what is being done to address them.
- The CISO's role is to become the board's trusted advisor. This enables the board to provide proper oversight and keep management accountable.

Dr. Anastassia Lauterbach
Professor and Author; Mentor
ExCo Leadership Group

Yaron Levi
CISO
Dolby Labs

Tim Rohrbaugh
CISO
JetBlue Airways

WSJ PRO CYBERSECURITY EXECUTIVE FORUM

Going After the Criminals

The Secret Service's main role in countering cybercrime is to ‘follow the money.’ Officers across the U.S. are coordinated from the agency’s Global Investigative Operations Center, effectively an ‘air-traffic control’ for cybercrime investigations, and the hub for collaboration with other law enforcement and government agencies.

Director James Murray said a big issue the agency faces is getting victims to come forward and report their loss in a timely fashion to allow agents to attempt to stop transfers and recover funds. Early reporting means the money can often be stopped in transit and returned immediately to the victim. If stolen funds cannot be stopped in transit, the agency seeks to seize money from criminals, which then goes into an asset forfeiture process. Returning money to victims via this method can take several months or longer.

To make the crime reporting process as efficient as possible, businesses should establish a relationship with their local Secret Service liaison officers before an incident so they know who to contact should the worst happen.

James Murray
Director
U.S. Secret Service

Lessons from a Cyberattack

After a ransomware attack in April, Ms. Duffy's executive recruitment firm paid a ransom of about $2,800 in bitcoin to get its operation-critical data back. The company negotiated the initial ransom demand down from roughly $30,000 dollars. Duffy Group was unable to restore all of its data.

In a business email compromise attack, Ms. William's nonprofit lost $650,000 after attackers compromised the email system of the nonprofit’s third-party bookkeeper. The attackers then inserted themselves into existing email chains by using similar email addresses to pretend to be people associated with the nonprofit.

Among the key takeaways:

- Have verbal confirmation before making a wire transfer to avoid being duped in a business email compromise attack.
- Build trust by being honest with customers about what occurred.
- Invest in cyber insurance coverage to mitigate losses.
- Small businesses may not get the help they seek by reporting the attack to authorities.

Kathleen Duffy
President and CEO
Duffy Group

Sherry Williams
Executive Director
One Treasure Island

How to Buy Cyber Insurance

Cindi Carter
Field CISO, Americas
Check Point Software Technologies

Ms. Carter shared some key takeaways that insurance buyers need to consider from a CISO perspective:

- Check that coverage extends to include breaches at third parties, including suppliers.
- Understand if sub-limits, liability exclusions or geographic limits apply to security incidents in the cloud.
- Check whether coverage applies retroactively, which could be important if a breach is subsequently discovered that took place before the policy was purchased.
- Know the communications process and key points of contact in the event of an incident.
- Maintain a dialogue with the insurer and communicate program improvements.

Robert Parisi
Head of Cyber Solutions North America
Munich Re

Mr. Parisi shared some key takeaways that insurance buyers need to consider from an industry perspective:

- Insurers have significantly evolved their approach to underwriting over the last few years due to the increase in costly ransomware attacks and supply chain risks.
- Premiums are rising while sub-limits, exclusions and deductibles vary widely.
- Buyers should expect to share more information about their exposure to cyber risk. Transparency about the organization's risk management and resilience efforts is critical.
- Insurers will respond well to applicants that treat cyber as an operational risk rather than simply trying to solve the challenge with technology.

WSJ PRO CYBERSECURITY
EXECUTIVE FORUM

WSJ Hosts and Moderators

David Breg
Deputy Research Director
WSJ Pro

Sara Castellanos
News Editor
The Wall Street Journal

Nicholas Elliott
Head of Professional Products Innovation and Strategy
The Wall Street Journal

Robert McMillan
Reporter
The Wall Street Journal

Kim Nash
Deputy Editor, WSJ Pro Cybersecurity
The Wall Street Journal

James Rundle
Reporter, WSJ Pro Cybersecurity
The Wall Street Journal

Rob Sloan
Research Director
WSJ Pro

Catherine Stupp
Reporter, WSJ Pro Cybersecurity
The Wall Street Journal

David Uberti
Reporter, WSJ Pro Cybersecurity
The Wall Street Journal

Dustin Volz
Reporter
The Wall Street Journal

WSJ PRO CYBERSECURITY EXECUTIVE FORUM

For in-depth cybersecurity news visit:
https://www.wsj.com/pro/cybersecurity

For cybersecurity research and event recordings, visit:
https://www.wsj.com/pro/cybersecurity/research

For upcoming WSJ Pro Cybersecurity events, visit:
https://cyber.wsj.com