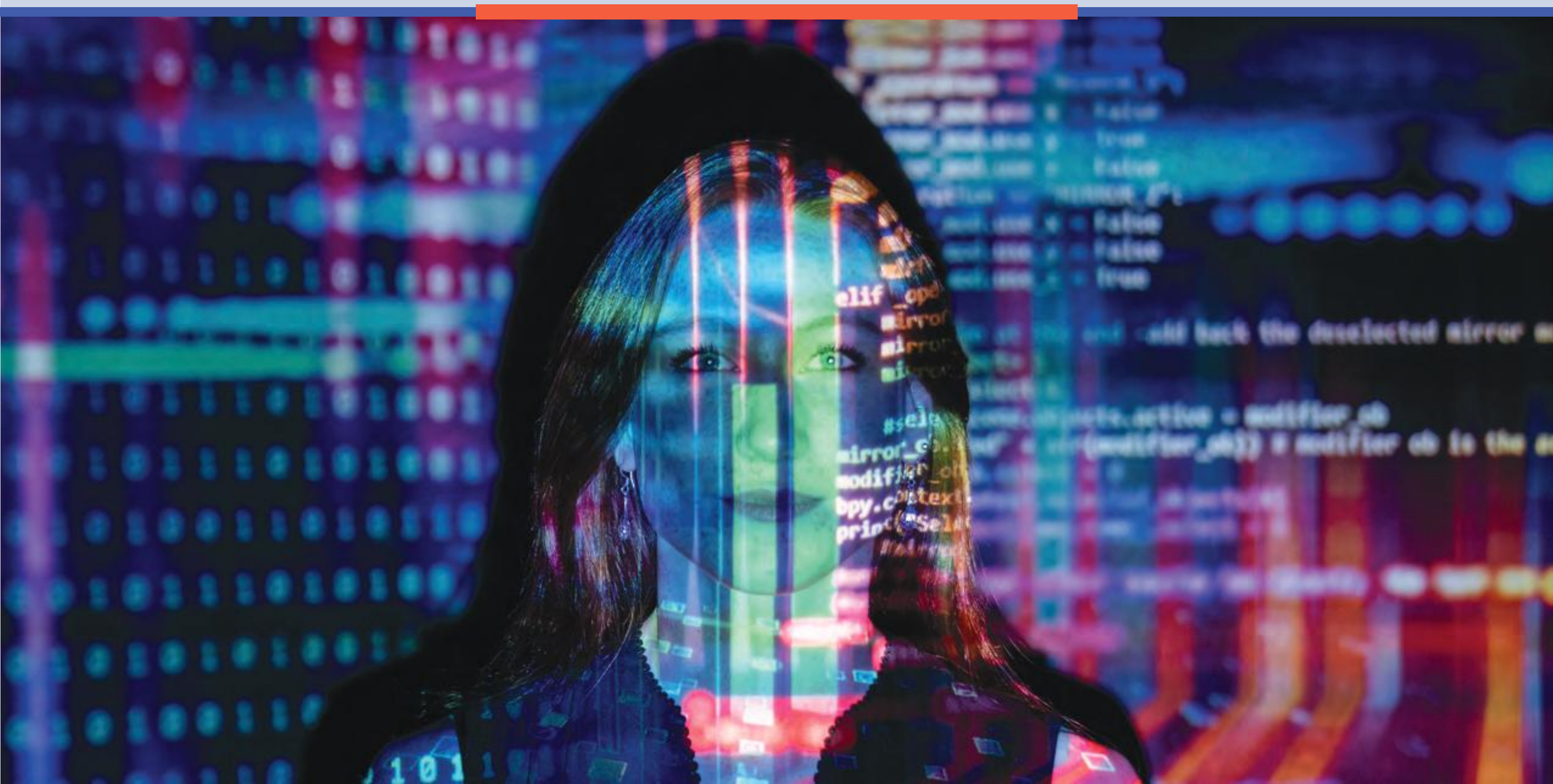
Cybersecurity - The Discipline of Vigilance



Cyberattacks are getting more sophisticated, more frequent, and more destructive – ranging from selling private customer data to shutting down critical businesses for ransom.

The war is being waged every day on every device on every service we use. Government institutions, software companies, retailers, public utilities have all been compromised. In a Cisco survey, 61% of respondents reported that their organization experienced a **jump of more than 25% in cyberthreats** since the start of Covid-19.

What are the tools and processes used to protect enterprise security? What does one do when security has been breached? What technologies and capabilities will drive the next phase of attacks and defense? What does this mean for entrepreneurs and investors?

A panel of industry leaders discussed these topics on August 10, 2021:

SAP

Tim McKnight, EVP and Chief Security Officer

SAP is a market leader in enterprise application software, touching 77% of the world's transaction revenue. Tim is responsible for SAP's overall security strategy and establishing SAP as a recognized and trusted leader in the industry.

FIS

Craig Conway, Global Head of Modern Banking Technology

FIS is at the heart of financial transactions, advancing the way the world pays, banks and invests; serving over 20,000 clients in over one million merchant locations, in over 130 countries.

SilverSky

Jason McGinnis, President & COO

SilverSky provides comprehensive cybersecurity solutions to thousands of customers, including those with strict security and compliance requirements such as financial institutions and healthcare.

Moderated by

SYNACOR

Himesh Bhise, CEO

Synacor, a cloud-based enterprise software company delivering collaboration, identity and advertising platforms

A Top Business Priority

Very public, large-impact attacks like Colonial Pipeline and SolarWinds, and recently T-Mobile (which became public after this panel). Geopolitical overtones. Enabling technologies like bitcoin. Increasing governmental and regulatory oversight. A standing board-level issue. The discipline of vigilance could not be more critical. Cybersecurity could not be a more visible priority in today's boardroom.

"Cybersecurity is a top business priority. It's a standing topic on a Board agenda. Threats can have a real kinetic effect - such as impacting life-support in a hospital. Threats can be about intellectual property theft and subsidizing your nation's interests by stealing the IP of others. It is more geopolitical than it has ever been, and it's become so lucrative that not-good actors are benefiting by holding companies to ransom," said Tim McKnight, Chief Security Officer of SAP.

"I think back to security protection we would offer to small financial institutions – it primarily included firewall and anti-virus. Flash forward 20 years – attacks are much more sophisticated, and the surface area of an attack looks like a block of swiss cheese. You have attacks from outside, inside, home-networks, bring-your-own broadband, IoT, every flavor of tablet and phone, add cloud and cloud computing – you get a much more complicated environment with more complicated attackers," said Jason McGinnis, President of SilverSky.

"What does it mean for the Cybersecurity function? It has received more investment and more board involvement. The amount of auditing has increased, and additional regulations have been imposed. We now need to ingrain security into the culture of the company, be secure by design, and drive continuing vigilance to stay current and stay one step ahead of an attack," said Craig Conway, Head of Modern Banking Technology at FIS.

Crippling Ransomware Attacks

The cost of Ransomware has been estimated at $20 billion in 2020. The average ransomware payout has grown to an estimated $234,000 per event, up 22% from a year ago, according to a report by Coveware. Many of these attacks also have geo-political overtones –a new arena of cyber-warfare, yielding political influence and accelerating nation-state technology progress.

Panelists shared their first-hand experiences - finding out that your IT systems have been hacked and your company held to ransom is scary and gut-wrenching, but too often can be a result of poor IT hygiene and planning.

Attacks can cripple your business Four thousand hacked files stalled transaction processing at a financial services company, resulting in major client impact. 70% of the network of an electronic medical records company was compromised – which directly stalled their ability to service customers. Attacks have moved to an extortion-ransom model - attackers are stealing files, encrypting those files, and then threatening to release customer data publicly, unless the ransom has been paid.

The "just pay it" philosophy emboldens attackers The financial company first elected to not pay ransom, tried to restore the system from backups, and realized that the file-backup had not been run for two weeks – leaving it with no choice but to pay up. The medical records company had no disaster recovery sites and had run no backups – after much internal debate had no choice but to pay the six-figure ransom.

- One panelist described a particular attacker that had hacked 47 companies and extorted $90 million in bitcoin – companies feel forced to pay, which in turn funds and emboldens bad-actors.
- Too often a company's strategy is to buy cyber-insurance rather than budget for security, not realizing the impact on enterprise value and customer relationships.
- Even if compromised files are returned by attackers, they may not be usable. The compromised financial services company spent days rebuilding systems from scratch even after paying the ransom.

Plain-Old IT Hygeine + A Standing Response Plan

Companies are required to abide by many compliance guidelines. These checklists can serve as a helpful baseline for protection, but too often companies are just 'checking the box'. Firewall – check, antivirus – check, security guidelines – check, even though the firewall hasn't been patched and the guidelines were written by a consultant two years ago.

Each business must define its own stance towards security based on the products it provides, the customers it serves, and the geographies in which it operates. It must incorporate the hygiene of defensive IT measures, as well as an agreed upon organizational response if a breach does occur.

Plain old IT hygiene reduces risk Security is critical to the function of enterprise today, and while it may never seem like one is doing enough, these processes are necessary to reducng risk:

- Preventative hygiene: Measures include running backups, using AI-based antivirus, installing up-to-date software patches, monitoring systems, updating collaboration tools (like Office 365) to prevent phishing attacks, and implementing identity and access management systems.

- Create-the-play, run-the-play: Study the cyber-attacks that have been published and match it against your defenses. Test and practice your response plan on a regular basis to stay prepared.

Every company needs a standing Response Plan

- Firebreaks: Using a forest-fire analogy, once malware has been introduced what are the technology and network architectures that can slow down an attack or isolate it before it spreads across the enterprise, creating time for the organization to respond.
- Communication: Understand requirements based on the business you're in, the geography you operate in, and the data that is potentially exposed. You don't want to communicate too early because it could be a false alarm, but you also don't want to communicate too late since that could be negligent. Stay coordinated with your lawyers, your media professionals, and your customer team, and stay on point.
- Professional negotiating help: Companies without in-house expertise can call experts to negotiate with hackers, set up the bitcoin wallet, and manage the process from payment to recovery.

Looking Around the Corner - Investable Growth Opportunities

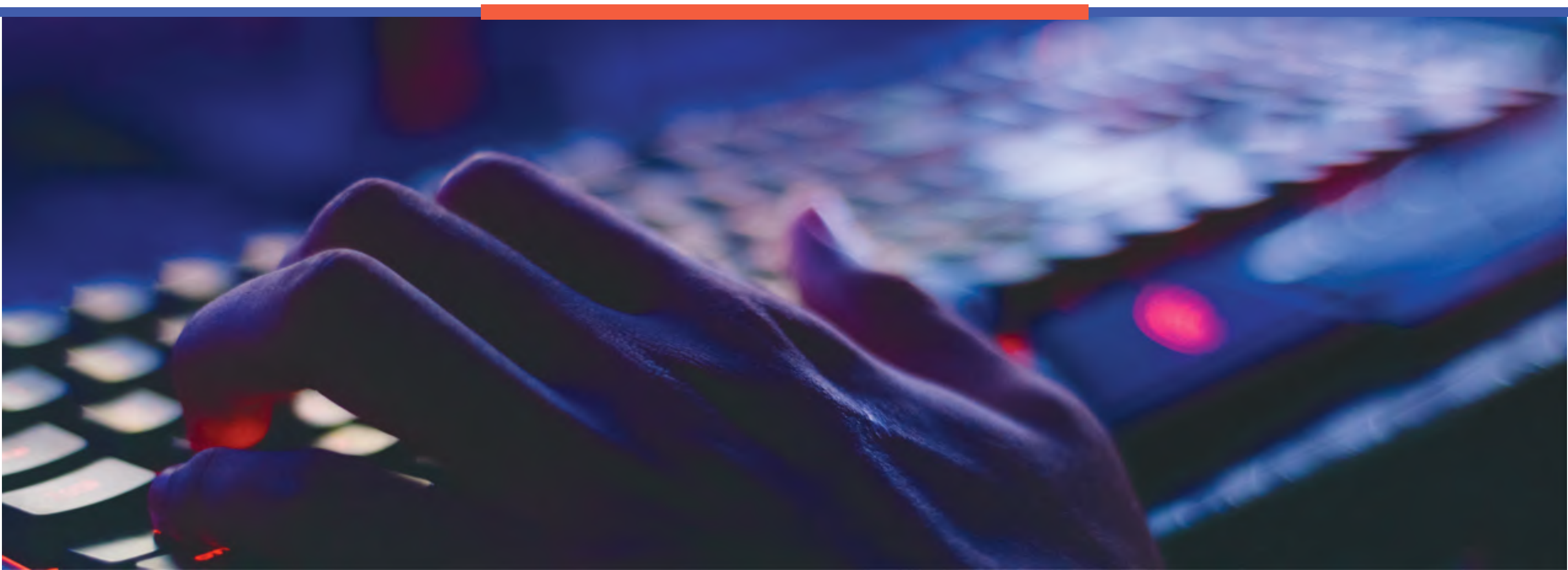
Analysts expect the Cybersecurity market to be close to $200 billion this year and growing. Some of the opportunities for investment surfaced by the panel include:

Security in the Cloud As more technology, applications, and corporate IT moves to the Cloud, configuring security and enabling access management in the cloud is becoming critical. It needs to run across the full stack, across a multi-cloud environment, and deliver health observability across these environments.

Real-time visibility of data Data now lives in a broader ecosystem of technology providers, SaaS products and partners. Currently companies do annual and bi-annual audits, but they are only a snapshot in time – not enough for where data proliferation is headed. Companies need easier, real-time tools to see how that data is flowing and how it is being transacted.

AI/ML driven security tools and data analysis Vast quantities of data are being produced, quickly expanding beyond traditional human examination. This data plays a critical role in analysis, threat-detection, automation, and constructing a security response. Artificial Intelligence and Machine Learning tools process that data and yield actionable outcomes in real-time.

Training There is a shortage in highly trained people. Enhanced training to drive security awareness, understanding risk, changing behavior, and putting controls in place.



Audacious ransomware attacks, geo-political overtones, privacy issues and regulatory oversight have made Cybersecurity a top business priority and a standing topic on Board-room agendas. Plain old IT hygiene – backups, antivirus, patching, monitoring, authentication – are critical to reducing risk and too-often overlooked. In addition, a standing organizational response plan that includes emergency procedures, stance towards ransom, and communication guidelines is essential to recovery. As data proliferates across platforms and the surface area of risk grows, investable opportunities appear to be in driving higher security across Cloud and multi-Cloud implementations; enabling real-time visibility into data produced across a company's ecosystem; using AI/ML tools to process that data and make it actionable; and creating expertise through better Training, necessary to maintain the essential discipline of vigilance.

From Market Disruption to Investable Growth

Panel discussions that bring together executives, entrepreneurs and investors, many from right here in Philadelphia, to discuss market disruption, first-hand experiences leading businesses and opportunities for investable growth.

Presented by TiE Philadelphia

Fostering development of the entrepreneur, entrepreneurship and the entrepreneurial ecosystem of Philadelphia, through mentoring, networking, education and funding

Author and Moderator: Himesh Bhise

Follow on Twitter @himeshbhise