BRANDED CONTENT

MAY 2, 2022

TECHTALK 2022

LOS ANGELES BUSINESS JOURNAL

SPONSORS

MILLER KAPLAN

Resecurity

USC Viterbi School of Engineering

TECHTALK 2022
LOS ANGELES BUSINESS JOURNAL

TechTalk 2022: A Roundtable Discussion

At a time when it is critically important for businesses to keep up with the latest technology trends – from mobility to cybersecurity to artificial intelligence – being ahead of the game can be a significant difference-maker in terms of a company's success. The right technical solutions up any businesses' game while engendering customer confidence and loyalty. Plus, protecting data, information, and communication has never been more essential as we all rely more heavily on technology than ever before.

The Los Angeles Business Journal recently assembled a panel of industry experts for the second annual TechTalk roundtable discussion. Moderated by Los Angeles Business Journal publisher and CEO Josh Schimmels, the panelists discussed common management mistakes and shared insights with the audience regarding how businesses should protect their systems, networks, and data from cybercrime and the Dark Web. The conversation also included updates on the artificial intelligence landscape and how to train the workforce of the future to prepare for such innovations.

Many thanks to these three thought leaders for sharing critical insights on what every business needs to know.

Yolanda Gil
Principal Scientist
USC Information Sciences Institute
Director, New Initiatives in AI and Data Science
USC Viterbi School of Engineering

"Academia and industry partnerships are crucial to solve AI challenges and to train students. Universities have multi-disciplinary experts, while companies have seasoned AI engineers working with rich data."

Kimberly Pease, CISSP
Director of Information Security Management Services
Miller Kaplan

"Without leadership, employees and IT staff will make their own decisions about securing information, which increases business risk and management is surprised to discover just how vulnerable they really are."

Gene Yoo
CEO
Resecurity, Inc.

"We are too far behind in time, resources, and funding to support on-going cyber security practices. Reducing technical debt and improving cyber hygiene will be key to improving cyber security postures for decades to come. Time to invest on right sizing security operations from top to bottom and acquiring solutions that protects the ecosystems of technology versus point solutions and commodity intelligence."

To view highlights from the virtual event, visit
labusinessjournal.com/events/techtalk2022

Resecurity

Reimagine Cybersecurity

Intelligence-driven security solutions.

- Big Data
- Dark Web
- Cyber Risk
- Threat Intelligence

www.resecurity.com | contact@resecurity.com

TECHTALK 2022
LOS ANGELES BUSINESS JOURNAL

AI-Powered Cybersecurity Protects Businesses from the Inside Out

If you open your news app of choice on any given day, you'll likely be reading about the latest cyber threat, ransomware attacks, hacktivists and most recently, nation-state actors launching attacks on the cyber battlefield.

While you might perceive this as a threat that would likely never impact your business, the reality is that cyberattacks on organizations increased by 50% in 2021. The same study revealed organizations in North America experienced an average of 502 weekly attacks per organization (a 61% increase).

The global pandemic, rise in remote work, reliance on e-commerce and increased geopolitical tensions have all driven this rapid increase, offering cybercriminals more opportunities and financial profits than ever before.

Most of these cybercriminals are financially driven, looking to steal data from enterprises and take their data "hostage" to leak it later, demand a sizable cryptocurrency ransom or monetize it by selling it on the Dark Web.

Beyond financially driven threat actors, state actors are becoming increasingly active, with more nation-state groups targeting high-tech corporations, scientific organizations, NGOs and government resources.

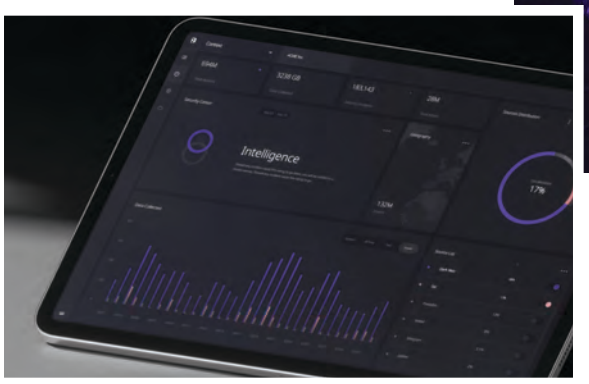
In what many are calling a 'cyber pandemic' or a new 'cyber battlefield,' businesses and enterprises must make data protection and threat intelligence a business priority. Accordingly, new AI-powered cybersecurity and threat intelligence software solutions have emerged to help enterprises secure their assets at scale and keep up with the ever-changing threatscape.

THE ROLE OF DATA PROTECTION IN TODAY'S WORLD

With data driving business practices and becoming more valuable by the day, data protection is no longer optional for enterprises. Data protection also extends to protect against accidental data loss and hacking attempts on your ecosystem. Protecting your enterprise cyber security makes good business sense: it protects against theft of sensitive information, accidental loss or destruction and other potential threats from malicious actors trying to gain access to valuable company data.

As a cybersecurity team that works with hundreds of organizations, Resecurity, an LA-based cybersecurity and threat intelligence company, has seen a spike in attacks against digital identity, including business email compromises and credentials spraying designed to steal or uncover re-used login credentials to gain access. Most of the time, these attacks lead to the compromise of remote access via SSO and VPN logins (originally designed to protect organizations) that ultimately allow the threat actors to penetrate the enterprise network and access critical resources.

However, you can't protect what you don't have visibility into. With the world creating 2.5 quintillion data bytes daily (that's 18 zeros), many businesses have trouble gaining visibility



into their data, digital ecosystem and the possible risks they're facing.

This is where cybersecurity and threat intelligence has come into play.

THREAT INTELLIGENCE AS YOUR SECRET WEAPON

Threat intelligence is a collection of data that provides information about the most common and latest threats you need to be aware of. It involves collecting and analyzing information about threats, such as hacker techniques, vulnerabilities in software, and exploits. When used correctly, threat intelligence allows an organization to be proactive and take steps to mitigate vulnerabilities before bad actors or hackers exploit them.

Resecurity is a pioneer of AI-powered threat intelligence solutions that organizations can implement quickly and at scale to protect their business. Resecurity's cyber threat intelligence platform, Context, accelerates analysis, prevention and investigation workflows with lightning-fast search and data science and contextualizes threat data to make it clear and actionable.

Through Resecurity, security teams can transform from managing many streams of raw intelligence and false positives to leveraging a single tool that provides a one-stop-shop for comprehensive threat intelligence data and real-time insights. By incorporating AI into their technology, organizations can decrease the time to identify cyber threats, save labor costs, reduce human errors and maximize their ROI.

The main goal of Resecurity's cyber threat intelligence platform is to give its customers early-warning notifications and increased visibility into threats targeting them, minimizing potential negative impacts. Resecurity has built one of the largest Dark Web intelligence repositories with over 3.4 billion records, and has cyber intelligence analysts deployed across all continents to gather the most relevant and actual data to help our clients protect their business.

Organizations who implement threat intelligence technologies minimize the risk of being breached by having actionable insights on their current threat landscape, new tactics, techniques and procedures (TTPs) of threat actors and real-time threat detection that allows their security or IT teams to respond before it impacts the business.

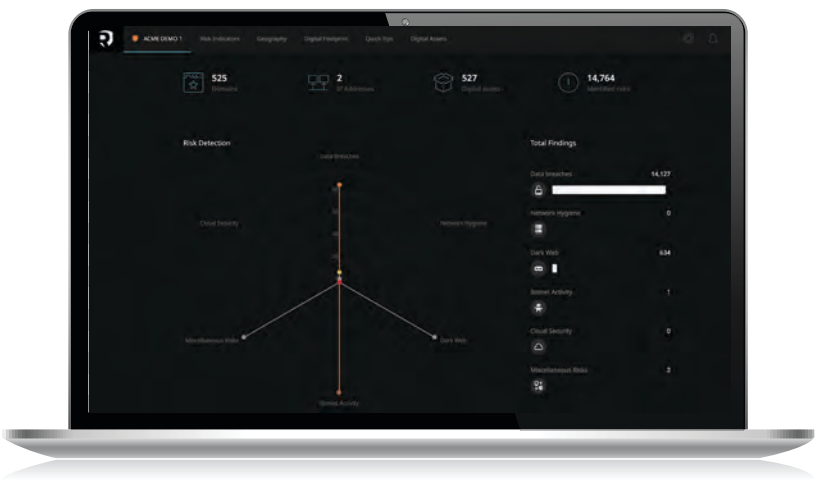
SECURING YOUR ORGANIZATION FROM THE INSIDE OUT

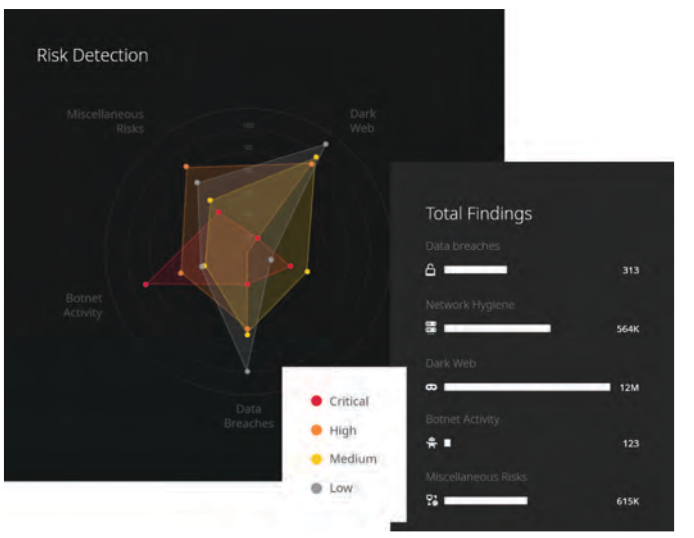
There is no question we will continue to see our digital landscape become the most prominent battlefield for criminals and nation-state actors. Today, business leaders and CISOs should focus on employee protection, remote access hardening and configuration security assessment to prevent network intrusions and data theft across the entire IT ecosystem.

Organizations that take advantage of threat intelligence will inherently enhance their security posture. When adding the layer of AI-powered threat intelligence systems that can pull information from far more sources than any human could analyze alone, enterprises can go beyond only responding to threats they already know about to proactively detecting and responding to threats they had no idea existed.

Like any other form of combat, having the right people, cybersecurity awareness training, intelligence and technology in place are essential to protect your organization on today's cyber battlefield.

Learn more at resecurity.com.





MILLER KAPLAN

It's more than just numbers. It's your business.

Ask us about our expert Information Security services.

We listen, then advise. This is why we are one of the top 100 certified public accounting firms.

MILLERKAPLAN.COM

TECHTALK 2022
LOS ANGELES BUSINESS JOURNAL

Managing the Business Risk of Securing Information

By KIMBERLY PEASE

One of the most common questions I hear executive leaders ask their IT departments is "are we secure?" Almost 25 years ago I had that same question asked of me when I held the position of CIO (Chief Information Officer) for a privately held manufacturing firm. Back then my answer was, "Yes, we are secure. We have firewalls and we changed the default passwords. We have backup tapes that we regularly take offsite. We have anti-virus installed and configured to run regular scans. And we have keypad access controls on the doors to the facility." I provided what I thought then was a knowledgeable, logical, and technically truthful answer; an answer we both accepted. We were confident, incorrectly, that that's what it meant to be secure.

Fast-forward to 2022 and the answer to that question is unequivocally and undeniably, "no." No business is secure if it has a connection to or a presence on the internet. And yet executive leaders are still asking the same question to IT personnel and getting the same answer: "Yes, we're secure." IT personnel confident in their skills and experience continue to provide a litany of all the technical controls in place. Both IT and executives still believe that it's the IT department's job to secure the business and keep the information secure.

Securing information, whether we call it "Information Security" or "Cybersecurity," is a business risk to be managed.

> Part of risk management means understanding how to respond when cyber incidents happen and preparing to be cyber resilient.

Executive leaders commonly pay keen attention to business risks such as financial, operational, regulatory, and competitive risk. But when it comes to cyber discussions they often defer to IT.

Cyber risk is just like any other risk to a business. Senior management must identify and convey its risk tolerance, not just to IT but to all employees. Risk tolerance represents the maximum risk that a company is willing to accept. The decisions surrounding whether to avoid, reduce, transfer, and even accept risk must first be made by senior leadership before appropriate controls and processes can be put in place for securing information. And while some IT vendors and IT practitioners may truly be doing an outstanding job of managing the security of the IT network on their own, most times executive leadership hasn't yet identified how much risk is tolerable before those IT security controls were put in place.

The overall risk management process methodically identifies risks surrounding your business activities which often includes using, storing, managing, and transmitting information. It includes assessing the likelihood of an event occurring. In today's cyber-threat landscape, it is highly likely that at some point the business and its employees will be a target by cyber attackers to get access to information or vital operational systems.

Part of risk management means understanding how to respond when cyber incidents happen and preparing to be cyber resilient.

Part of managing cybersecurity risk is identifying laws, regulations, and contractual requirements the business may have to comply with. Managing cyber risk is enforcing adherence to overall cyber security programs, industry frameworks and policies and standards. It includes identifying roles and specific responsibilities designated by executive leadership and creating a team of subject-matter-experts.

It requires an all-hands-on deck approach involving culture, education, and guidance to employees on how to handle information.

Organizations that are effective at managing the security of their information have three behaviors setting them apart from others. First, the highest-ranking executive of the firm makes information security governance a priority and enlists the support of information security management experts. Second, they take a risk-management approach to information security incorporating appropriate formal, risk-driven industry frameworks. And third, they govern IT in accordance with clear IT security standards.

Without executive leadership and guidance, employees and IT staff will make their own decisions about securing information; decisions which often increase business risk. Then executive management is surprised to discover just how vulnerable they really are. Unfortunately, they often discover this after a cyber incident occurs – which is too late.

So, the next time you think about asking IT "are we secure?" – instead ask yourself: "As the highest-ranking executive, how much information risk am I willing to tolerate and who should I have in the room to help me identify what controls and processes to have in place?"

Kimberly Pease, CISSP, is director of information security for Miller Kaplan. For more information, visit millerkaplan.com.

The Insecurity of Everything: A Look at the Reality of Hard Drive Destruction

By KATE FAZZINI and JOHN SHEGERIAN

As a business leader, it's your responsibility to ensure that your clients', workers', or associates' private information is kept confidential. Many are not aware of the intricacies of recycling electronics in a way that completely destroys data.

JUST BECAUSE YOU'RE NOT REQUIRED, DOESN'T MEAN IT'S WORTH THE RISK

The FTC's Disposal Rule requires information that's used in consumer records and reports to be correctly disposed of. The rule is in place to eliminate the risk of "unauthorized access or use of the information." The Disposal Rule covers the organizations and businesses that must follow this rule. They include:

- Anyone who pulls credit reports, such an individual hiring caregivers
- Banks, lenders, debt collectors, and other financial companies
- Consumer reporting agencies and credit bureaus
- Employers
- Government agencies
- Insurance agents and companies
- Landlords and property management firms
- Lawyers and law firms
- New and used car dealerships
- Private investigators

You also have HIPAA rules protecting patient information. Doctors, medical offices, nurses, etc., must be conscientious that this confidential information is appropriately disposed of. Proper disposal is defined as:

1. Burning, pulverizing, or shredding paper documents
2. Destroying or erasing electronic files and devices to prevent the information from being read or recovered

The best practice is to err on the side of caution. If there are any papers or files you have for clients that could contain private information, it's best to dispose of them properly.

DON'T ASSUME YOU WILL NOT BE PART OF A THEFT

Worldwide, businesses and organizations lose about $1.8 million every minute to cybercrime. More than half a million records were compromised. The average cost of a breach is more than $7 per minute.

You can't assume you're safe. You may not think your business has information that's valuable to someone else, but what if you are wrong? What if the addresses and phone numbers you store are valuable to a scammer? Do you want to risk your reputation on a theft that you could have prevented by destroying data and recycling your electronics?

To be proactive, hire experts in data destruction. If you eliminate the chances of private information being stolen from unused or outdated electronics, you reduce potential cybercrime against your company or organization.

DON'T THINK THAT ONLY COMPUTERS REQUIRE DESTRUCTION

Computers are not the only electronics that you should destroy. All kinds of office and home equipment can store private information. A printer keeps a record of the things you print out. If it's a multi-function printer, it holds everything you copy and print out. Fax machines also store images that are sent or received.

If you're only sending your computers to a company to have the data destroyed, you could be making a big mistake. You must destroy data on phones, fax machines, printers, copiers, cash registers, imaging machines, etc.

DON'T THINK YOU CAN JUST PULVERIZE AND THROW AWAY BROKEN ELECTRONICS

One of the biggest misconceptions we hear is that it's okay to throw out electronics after breaking up a hard drive. If you smash it into pieces so that it is beyond repair, it's okay to trash it.

This is the most irresponsible thing that can happen. While many states do not have specific laws against throwing away electronics, the EPA does have laws against hazardous waste disposal. Electronics contain heavy metals like lead and mercury. They have plastics that don't break down in landfills. They also have gold, silver, copper, and many other metals. Those metals and toxins can seep into the soil and groundwater and cause irreparable damage to people and animals.

CAREFULLY CHOOSE YOUR ITAD PROVIDER

How do you know if you're partnering with a responsible, effective data destruction provider? Look for providers who specialize in both IT asset disposition (ITAD) and data destruction. ITAD providers can help you destroy data following the level of data destruction your business requires. They can help you remarket any electronics that still have value, enabling you to recover the cost of ITAD services. You also want a company that focuses on a low carbon footprint to protect the environment.

Kate Fazzini is director of security operations and engineering at Ziff Davis; and an adjunct professor of cybersecurity at Georgetown University.

John Shegerian is co-founder and Chairman/CEO of ERI, the nation's leading fully integrated IT and electronics asset disposition provider and cybersecurity-focused hardware destruction company.

TECHTALK 2022
LOS ANGELES BUSINESS JOURNAL

New Open Radar API Standard is Launched

Earlier this year at CES 2022, the Consumer Technology Association (CTA) announced Ripple, a new industry standard for radar system development that will enable hardware and software interoperability for general purpose consumer radar across industrial, automotive and medical applications. The new standard was a collaborative effort led by CTA's Ripple Technology Project Group with participation from industry leaders including Aptiv, Blumio, Ford, Google, Infineon, NXP, and Texas Instruments. The industry-led group formed in early 2021 to accelerate the growth of low-power, general purpose radar.

Radar sensing systems have historically been designed for single applications, with hardware and software custom-developed for each purpose. This means that traditional product solutions — from the hardware to the final user experience — are bespoke. This new standard will enable general purpose radar interoperability by developing both specifications for open and standardized application programming interfaces (APIs) and a collaborative plan to drive industry adoption of the standard.

"Our standard will encourage radar interoperability, allowing our industry to harness the power of this technology in innovative ways," said Kerri Haresign, director of technology and standards at CTA. "This standard has meaningful benefits for consumers and industry drivers across the globe. From home security systems to hands free operation of devices in our vehicles and homes, radar interoperability will lead to better products for consumers and faster innovation around the technology. We are proud of the work our members undertook on this industry-led effort and look forward to expanding the API to include additional radar waveforms and features."

"Ripple will unlock helpful innovation that benefits everyone," said Ivan Poupyrev, Director of Engineering and Technical Projects Lead, Google ATAP. "General purpose radar is a key emerging technology for solving critical use cases in a privacy-respecting way. We are excited to contribute and collaborate with the other members of the technical project group and the technology industry more broadly. We welcome more companies and developers to reach out and participate in Ripple."

The benefits of a general-purpose radar API include:

- **New products and services for consumers:** Radar enables features like non-invasive wellness monitoring; detection of unusual inactivity in a home, which can be a sign that someone needs help; nonverbal gesture recognition on devices, like a simple wave of your hand changes the song on your phone; and hands-free operation of things like car doors.
- **Interoperable software libraries:** With standardized calls, software libraries can work across various radar hardware implementations, ensuring reusability and easier firmware upgrades.
- **Growth of radar hardware ecosystems + integrators:** With an open API standard, it's easier for integrators to get started, develop and distribute radar solutions. This reduced barrier to entry will lead to new products and services for consumers.
- **Opportunities to innovate and differentiate with extensions:** Ripple will enable developers to create specialized extensions so that they can build on the standard to support their own differentiated use cases. These extensions can be incorporated as official interfaces in future versions of the standard.
- **Education and academic research:** Standardized software that works across all radar applications can simplify experimentation and prototyping; making radar more accessible to students, startups, academics and researchers.

CTA's members are the world's leading innovators – from startups to global brands – helping support more than 18 million American jobs. CTA owns and produces CES – the largest and most influential tech event in the world.

Learn more at CTA.tech.

TECHTALK 2022
LOS ANGELES BUSINESS JOURNAL

New Directorate for Technology, Innovation and Partnerships is Launched

Last month at SXSW 2022, U.S. National Science Foundation (NSF) director Sethuraman Panchanathan announced a new directorate within the NSF focused on Technology, Innovation and Partnerships, or TIP, during his session on Reinvigorating Science and Technology for the Future of U.S. Innovation. This new directorate — NSF's first in more than 30 years — builds upon the agency's commitment over seven decades to serve as a beacon of U.S. innovation, advancing the frontiers of research and education across all fields of science and engineering. TIP is a critical first step that will accelerate the development of new technologies and products that improve Americans' way of life, grow the economy and create new jobs, and strengthen and sustain U.S. competitiveness for decades to come.

"NSF's TIP Directorate will accelerate discovery and innovation to rapidly bring new technologies to market and address the most pressing societal and economic challenges of our time," said Panchanathan. "By pursuing new approaches that engage the nation's broad and diverse population in shaping research directions and outcomes, TIP will be a game-changer in terms of the pace of technological breakthroughs, future job growth and national competitiveness. We at NSF are grateful for the continued strong support from the Administration and Congress that has made this possibility a reality. We look forward to the passage of the Bipartisan Innovation Act, which will be the next critical step in ensuring TIP can generate a transformational evolution in translating America's research to expand our economic leadership in the technologies of the future."

Through TIP, NSF plans to launch a set of integrated initiatives. Together, these initiatives will advance critical and emerging technologies; accelerate the translation of research results from the lab to market and society; and cultivate new education pathways leading to a diverse and skilled future technical workforce comprising researchers, practitioners, technicians and entrepreneurs. This will no doubt expand the geography of innovation and help deliver on NSF's Missing Millions goals.

Notably, over time, TIP will establish regional "innovation engines" throughout the U.S. These innovation engines will advance use-inspired research, entrepreneurship, and workforce development to nurture and accelerate regional industries, ushering in a transformational revolution of business and economic growth regionally and nationally that strengthens bottom-up, middle-out growth in industries and communities across America.

The TIP Directorate will leverage strategic partnerships spanning multiple disciplines and sectors to advance the frontiers of emerging industries, from trustworthy artificial intelligence systems to biotechnology, cybersecurity, next-generation wireless networks, microelectronics and semiconductors, and quantum computing platforms.

TIP will also extend the opportunities of science and technology to every American, establishing both a broad footprint that touches communities across the country and novel education pathways available to anyone who wishes to pursue new, high-wage, good-quality jobs in science and technology. TIP is a critical element of NSF's support for future science and technology leaders who reflect the rich cultural and geographic diversity of the U.S. — one of the nation's greatest advantages in global competition and leadership.

In addition to new investments, NSF is repositioning much of its existing innovation and translation portfolio into the TIP Directorate, including the NSF Lab-to-Market Platform comprising the NSF Innovation Corps (I-Corps™), Partnerships for Innovation, and America's Seed Fund powered by NSF programs, as well as the NSF Convergence Accelerator.

NSF has selected Erwin Gianchandani to be the inaugural NSF assistant director for technology, innovation and partnerships, leading the new directorate. "Gianchandani is a visionary leader with a wealth of experience in research, innovation and partnership programs," said Panchanathan.

NSF will provide more information about TIP opportunities and partnerships as the directorate grows its existing programs and establishes new ones.

The NSF supports research and people by providing facilities, instruments and funding to support their ingenuity and sustain the U.S. as a global leader in research and innovation.

For more information on the TIP Directorate, visit beta.nsf.gov/tip/latest.