AMERICAN BANKRUPTCY INSTITUTE

2020 ABI Health Care Program: The New Reality in Health Care

Cybersecurity Attacks: What Keeps You Up at Night

David Breg, Moderator
WSJ Pro; Princeton, N.J.

Matthew Dunn
Kroll; Nashville, Tenn.

Joey Johnson
Premise Health; Nashville, Tenn.

Roy Wyman
Nelson Mullins Riley & Scarborough LLP; Nashville

2020

WSJ PRO RESEARCH

WSJ PRO CYBERSECURITY

Managing the Mental Health of CISOs and Their Teams

By Marilia Wyatt, Cyber Risk Analyst, WSJ Pro Research

The mental stress associated with keeping networks secure from constant attacks is affecting chief information security officers and the teams they manage. Left unchecked this stress could significantly affect a CISO's mental wellness and security staff retention rates—both of which could negatively affect an organization's cybersecurity.

The job-related stressors are well documented:

- Feelings of personal responsibility for breaches.
- Long hours and being 'always on.'
- Job insecurity in the case of a compromise.
- Understaffed teams running on the maximum bandwidth.
- Slim budgets resulting in unrealized security projects.
- Disillusionment stemming from security often being viewed as an afterthought.
- Constant pressure to learn and monitor changes in risk and threat.

CISOs are not unique among executives in having to deal with high stress, but they might be at higher risk due to their personal investment in an organization's security. This, in turn, can lead to an increased risk of burnout, depression, fatigue, anxiety, substance abuse, and even suicide risk—all concerns that businesses will need to grapple with, rather than sweep under the corporate rug.

> "We are behind computer screens for 12 hours or more at a time often without human interaction. The social isolation can cause depression and you think you are the only one having to deal with certain issues. Twelve people I personally knew have died by suicide."
>
> Amanda Berlin, chief executive of Mental Health Hackers, a non-profit that works to remove the stigma of mental wellness challenges for security professionals.

Build Mentally Resilient Teams

Jamil Farshchi, chief information security officer at Equifax Inc, speaking at the December 2019 WSJ Pro Cybersecurity Executive Forum in New York, recounted the effects on cybersecurity staff of a 2014 data breach at Home Depot Inc., where he used to be CISO. "You have a workforce that's been grinding day-in, day-out for several months, and I'm talking about situations where people have put cots on the floor and are staying there night after night," Mr. Farshchi said. "What you step into, when you get into an organization that's post-breach, is chaotic."

The prolonged stress levels cybersecurity teams experience can potentially affect how a company maintains resilience, not only affect their well-being. Dr. Ryan Louie, a psychiatrist at Vituity, a multispecialty partnership of physicians, said mental health can affect how a company counters threats. "The risks to companies are the lingering effects after and during a cyberattack that affect a workforce's ability to respond and maintain resilience and upkeep that constant alertness and ability to perform well in times of extreme stress."

According to a survey from the U.K. domain name registry Nominet, 88% of CISOs said they were "moderately or tremendously stressed." Of the 406 CISOs or similar roles surveyed, 48% reported stress levels affected their mental health, up from 27% last year. Ninety percent reported they would take a pay cut to achieve work and life balance and 31% said stress affects their ability to do their job.

The 2020 Nominet report didn't go into specific mental health risks, but raises questions about the long-term effect of stress on the CISO and the organization's security posture. The leaders said they are expected to work long hours—an average of 10 hours extra per week beyond contracted hours--that results in missing family and social time.

48% of CISOs reported stress levels affected their mental health.

U.K. domain name registry Nominet

Culture Matters

A company's culture is important to reduce stress, said Nominet's CISO, Cath Goulding. "It makes my job easier when we are all working towards the same goals, and I can make security fit into that."

"The CISO stress is different in that they generally have bad news about incidents and need to ask for money to mitigate risks," Ms. Goulding added. She points to mindfulness courses and yoga, both available at the company, that help her take a step back from work.

There is a cost associated with any worker being absent from the office for a period with stress-related illness, but the loss of the CISO for a longer period could potentially affect the company's cybersecurity.

The Cost of Recruiting CISOs

According to Deidre Diamond, CEO at CyberSN, a cybersecurity staffing company, the average tenure of CISOs is 18 months in the U.S. and two years overseas. The Nominet survey, largely based on data from U.K., found the average CISO tenure is 26 months. The high turnover rate of CISOs means companies are already exposed to regular periods without a security leader. Investing in mental wellness could help keep a CISO in place for longer while avoiding the costly and oftentimes difficult recruitment of a replacement.

"The CISO role takes an agency on average eight months to fill. The larger the company, the longer the process."

Deidre Diamond, CEO at CyberSN, a cybersecurity staffing company.

The Tone at the Top

A company's cybersecurity resilience is only as strong as the endurance and vitality of its people, combined with its technical capabilities. A robust cybersecurity immune system means a workforce can quickly recover from stress and perform at an optimum level to keep the organization secure. The responsibility for building that resilience and ensuring the well-being of the team lies with the CISO, or equivalent security executive.

The CISO must set the tone continuously, which includes taking their annual leave and not expecting others to forego their leave. Team members must be encouraged to make use of mental wellness assistance offered by the organization and foster an environment and culture where stress is not perceived as weakness. Being sensitive to the team's emotional diversity to gauge how the work affects them differently, depending on other personal challenges, will also be a skill for the security leader to develop.

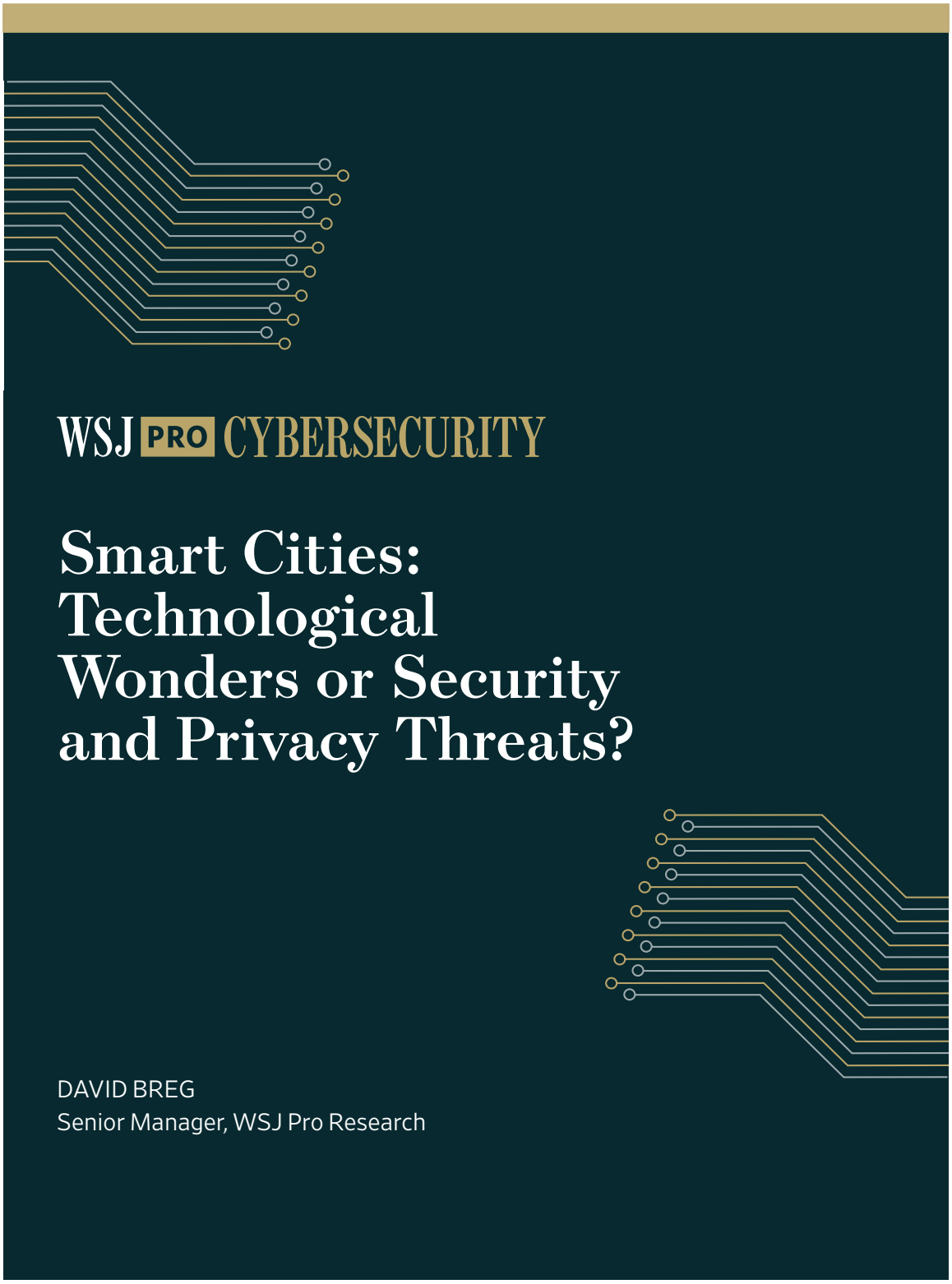
What Can Companies Do?

There are a number of steps organizations can take towards a healthier work environment, without affecting the ability of the cybersecurity team to deliver against risk and security goals:

- Evaluate the current mental wellness resources. If a corporate-wide program is in place, is it sufficient to cover the cybersecurity department's particular needs?
- Work with HR to understand whether stress has contributed to staff absences or was a factor in cybersecurity team retention rates.
- Discuss how stress affected the effectiveness of responses to previous incidents.
- Identify those roles that are exposed to prolonged stress levels. Consider rotating workers to reduce stress on individuals. Ensure all team members take annual vacation days.
- Provide senior managers mental health first aid training to help gauge when teams are struggling. Give thought to a mental wellness ambassador for the cybersecurity team.
- Offer counseling opportunities on-site and off-site that fit cybersecurity workers' schedules.

Marilia Wyatt is a cyber risk analyst at WSJ Pro Research, The Wall Street Journal's professional arm. Marilia writes research and analysis, develops strategy, and creates solutions to augment executive decision-making around improving cybersecurity, data privacy, ethics, and responsible use. She's got a passion for building things that provide utility for readers and leverage innovation with the responsible use of technology.

Submit research ideas or feedback to marilia.wyatt@wsj.com


WSJ PRO CYBERSECURITY
Smart Cities: Technological Wonders or Security and Privacy Threats?
DAVID BREG
Senior Manager, WSJ Pro Research

WSJ PRO CYBERSECURITY

Smart Cities: Technological Wonders or Security and Privacy Threats?

Executive Summary

Population growth, combined with increasing numbers of people moving to cities, is driving a need for more sophisticated methods to house, transport and protect people while alleviating the strain on natural resources and the environment. Concurrently, the development of leading-edge technologies with the ability to process and analyze massive volumes of data is creating an opportunity to more efficiently manage infrastructure and safety needs.

Harnessing these technologies and applying them in an urban setting has resulted in the development of "smart cities" that many hope will be the solution to the needs of growing urban populations. Businesses, in particular, will likely benefit from smart cities via improved buildings, transportation options and cost savings, with the companies involved with smart city construction activities expected to profit from their contributions.

But while the ability to enhance sustainability while delivering services and providing greater conveniences to individuals are admirable—and necessary—goals, important concerns are also associated with smart cities. Security breaches have already disrupted transportation systems, utilities and 911 services and the goal of linking smart technologies through a single network to increase efficiency also raises the specter of multiple services that could be shut down via a single point of entry.

Every person living in a smart city produces reams of data over the course of a day and the networks that compile and monitor this information present the possibility for insiders to misuse the data, including such activities as spying or selling personal data for illegal gain. Security and privacy advocates have expressed their concerns about how smart cities are constructed and how the information they produce is used.

> "Smart city is a concept born in the late '90s describing the digitalisation of urban information and the potential to apply artificial intelligence to information collected through sensors, to give timely responses to metropolitan problems."
>
> **Dr Sara Degli-Esposti**
> Research fellow at the Centre for Business in Society at Coventry University [1]

The goal for everyone involved is to find a balance that allows government officials to proceed with their smart city plans, while respecting citizens' needs for security and privacy. Making this goal more challenging is that currently there are few regulations and little oversight regarding security and privacy. A glimmer of hope is that use cases and best practices are starting to emerge and associations of smart city practitioners have been developed and are adding new members at a steady pace.

Preliminary research indicates that while individuals are concerned about how their personal information and data are used, most are willing to give up some of their privacy in return for the conveniences and gains to be had from smart city technologies. This flexible approach is probably for the best, as several hundred cities have already started smart city projects and the forward momentum, along with the need for the efficiencies smart cities provide, will almost certainly continue and grow.

[1] South China Morning Post, 15 August 2018

Introduction

The notion of a "smart city" conjures various thoughts among different people, including favorable terms such as innovative, visionary, ultramodern and, most optimistically, "futuristic urban utopia,"[2] along with more negative thoughts like "tech for tech's sake" and "big brother is watching." There is a certain degree of logic behind all of these descriptions, with many observers acknowledging both the benefits and risks associated with smart city projects.

An individual's attitude toward smart cities is likely influenced by her or his level of comfort with technology, as well as the person's feelings toward privacy and security. The key, most would acknowledge, is to find the appropriate balance between these competing benefits and concerns, with education, sharing of best practices, open discussion and input from citizens being important factors for bridging the differences.

The definition of a smart city and what it consists of may vary, depending on who you ask, but most usually highlight such factors as the use of digital technologies to transform living and working environments, using infrastructure (e.g., transportation, buildings) more efficiently and using technologies to engage local people.[3] Reducing resource usage, waste and costs are typically leading goals of most smart cities.

This paper provides an overview of the needs for and key features of smart cities, including the status of smart city development and ways in which businesses can benefit. It also addresses the security concerns, including examples of cybersecurity attacks that have already impacted the safety and well-being of individuals, and the privacy issues that are being debated between city planners and privacy advocates. Finally, the paper includes a review of best practices and potential solutions for security and privacy needs.

Changing Demographics Driving Growth

An important force behind the development of smart cities is the rapidly growing urban population across the planet. More than half (54%) of the world's population of 6.8 billion currently resides in urban areas compared with just 30% in the 1950s.[4] Or looked at another way, the current 3.7 billion urban residents are more than the total world population prior to 1970.[5] By 2050, fully 66% of global citizens will be urban dwellers.[6] **This increasing movement toward cities will create myriad challenges, including traffic congestion, threats to water and air quality, and risks to digital security.**[7]

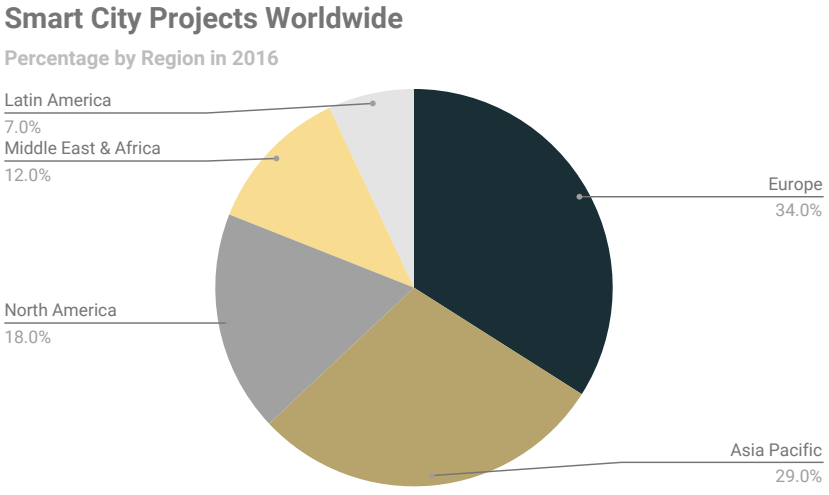
> There are currently 21 Megacities with a population of more than 10 million. Prior to 1975 there were only three.[8]

Examples of cities that are addressing these challenges by adopting smart city principles include New York, Singapore and Amsterdam, which were highly rated across several key smart city categories in a June 2018 report by McKinsey, including their ultra-high-speed communications networks and plans to launch 5G services.[9] However, the number

[2] MIT Press
[3] Cities Digest, 23 May 2017
[4] Trend Micro: Securing Smart Cities
[5] Worldometers
[6] Trend Micro: Securing Smart Cities
[7] Voice of America Press Releases and Documents, 15 November 2018
[8] Postscapes, 4 May 2018
[9] McKinsey Global Institute, June 2018

of cities adopting various forms of smart city technologies is much greater. European Parliament research from 2017 claimed that region already had 240 cities with populations over 100,000 that have some smart city features in place,[10] while estimates suggest there are more than 450 cities globally that have adopted at least one smart city project.[11]

Most smart city projects are driven by the mayors or councils of each city, but an exception is India, where a national initiative calls for cities around the country to develop smart city programs. Prime Minister Narendra Modi launched the Smart Cities Mission in 2015 with the goal of developing an area within 100 cities to serve as models for developments in other areas of those cities.[12] Financial aid is being provided by the federal and state governments between 2017–2022 to all of the cities, with results expected from 2022 onwards.[13]



Source(s): Siemens; Navigant Consulting

[10] Smart Cities World, 23 January 2019
[11] Computer Weekly, July 2018
[12] The Indian Express, 14 June 2017
[13] CB Insights, 9 January 2019

High Costs, But Potentially Greater Savings

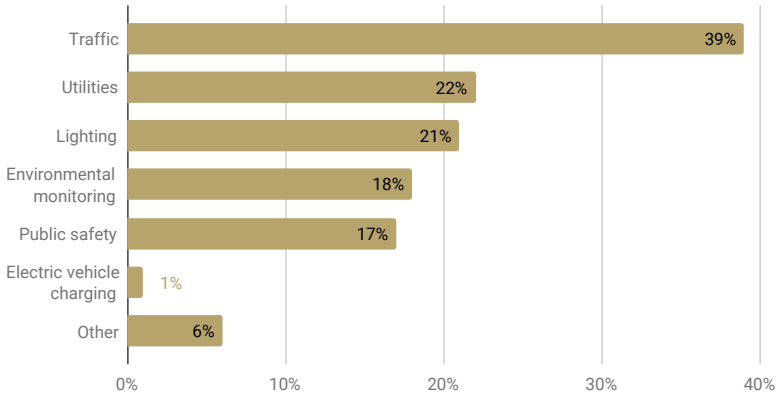
The economic impact of smart cities growth is potentially significant, although a disparity of estimates on current and future spending presents a challenge in making a reliable analysis. One prediction values overall spending at $80 billion this year and rising as high as $135 billion by 2021,[14] while another estimate expects smart city investments to grow from $36.8 billion in 2016 to $88.7 billion by 2025.[15] Complicating matters are estimates that focus more broadly on investments in the Internet of Things (IoT) tools and platforms to modernize cities around the world, with a prediction that these components will exceed $2 trillion by 2025.[16]

While the costs associated with developing smart cities are large by any estimate, the cost savings—monetarily, as well as from a resource and environmental perspective—are potentially much greater. A white paper by ABI Research forecasts $5 trillion in savings annually for smart cities globally by 2022. Factors such as "reduction in operational costs" and "faster and more efficient decision making" were cited in a survey of companies as reasons for the cost savings, while technologies such as automation, artificial intelligence (AI), sensors, data sharing and analytics will be critical in helping cities reduce costs.[17]

> "Currently most smart city models provide solutions in silos and are not interconnected. The future is moving toward integrated solutions that connect all verticals within a single platform. IoT is already paving the way to allow for such solutions."
>
> **Vijay Narayanan**
> Visionary Innovation Senior Research Analyst at Frost & Sullivan[18]

Distribution of Smart City IoT Projects Worldwide

By Segment, January 2018



Source: IoT Analytics. Total exceeds 100% because a project may be applicable to more than one category.

[14] ZDNet , 9 August 2018
[15] Trend Micro: Securing Smart Cities
[16] The Recorder, 24 October 2018
[17] ABI Research: Smart Cities and Cost Savings, December 2017
[18] Marginalia, 4 June 2018

Implications for Businesses

The positive effects of smart cities on businesses include the direct impact for companies involved with building the infrastructure that will enable smart cities to happen. The monetary incentives for these companies are significant, as **smart cities are anticipated to create business opportunities with a market value of over $2 trillion by 2025**. There will also be indirect benefits the technologies associated with smart cities will afford businesses generally. AI, personalized health care, robotics, advanced driver assistance systems (ADAS), distributed energy generation are technologies business consulting firm Frost & Sullivan believes will be the cornerstones of smart cities of the future.[19]

Another tangible benefit smart cities may offer businesses is the ability to **leverage the data being collected** by the smart city to better understand their target demographic and the space itself to provide a more targeted service. For example, the data generated by visitors can help businesses in the tourism industry understand patterns in mass-transit delays and the typical wait times for passengers. This will enable a service like the Citymapper app, which can use Transport for London's data to assist passengers with planning trips and finding the quickest routes in London.[20]

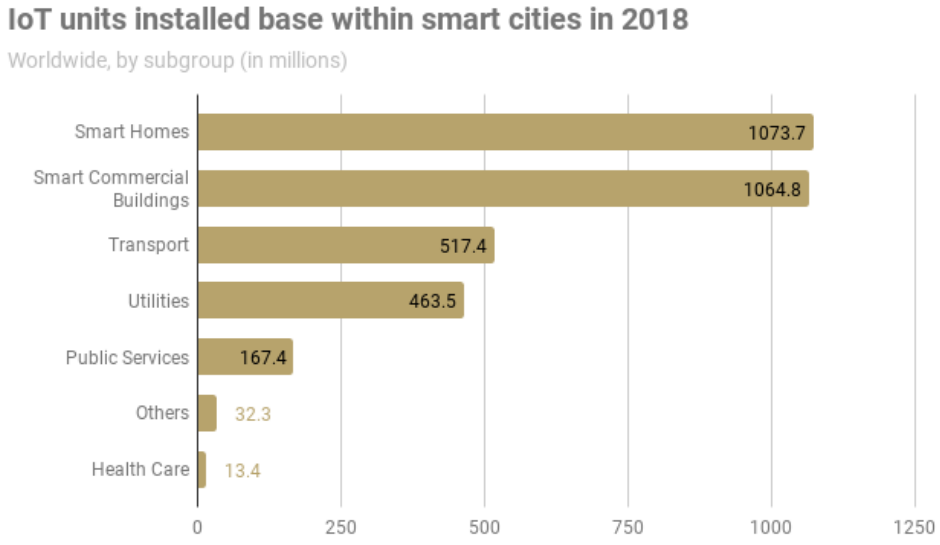
Another opportunity smart cities offer businesses is the capability of **enhancing their Environment, Social and Governance (ESG) credentials** by contributing to, or operating within, smart cities. According to a 2015 Nielson study, 66% of respondents indicated they would pay a higher price for a product or service if the company showed a commitment to positive social and environmental change.[21] As consumers' demand for sustainability grows, businesses operating in a smart city model will likely see improved relations with customers, with rising profits as a potential byproduct.

Smart buildings can be a **recruiting tool** for companies by making the workplace more efficient and comfortable for their workers, along with the appeal and status of working for a forward-looking company. Businesses will be attracted to the efficiency of devices such as smart heating/cooling and smart lighting that will result in cost savings.[22]

> *"Smart technologies change the nature and economics of infrastructure…The result is not only a more livable city but also a more productive place for businesses to operate."*
>
> **McKinsey Global Institute**[23]

[19] Marginalia, 4 June 2018
[20] Innovation Enterprise, 15 January 2018
[21] Nielsen, 12 October 2015
[22] Innovation Enterprise, 15 January 2018
[23] McKinsey Global Institute, June 2018

A challenge for businesses is understanding how to interact with municipal governments attempting to develop smart cities. Historically, "serving a city" involved selling a product or service directly to city governments, but the dynamic is changing with smart cities. Companies will need to understand the context and complexities of each city's plans and develop a long-term strategy for engaging with municipal leaders. Sales teams may need to expand their capabilities and skill sets with assistance from experts in such fields as sociology, urban planning and design to help broaden their thinking. An example of this adaptive approach involves Siemens and its London-based Center of Competence for Cities, where a broad array of specialists, including experts in urban planning, public finance and architecture, are employed in multidisciplinary teams.[24]



Source(s): CSI Magazine; Gartner

This chart represents the installed base for Internet of Things devices within the smart cities segment in 2018, with a breakdown by subgroup. Analysts forecast over one billion connected devices will be installed in smart homes.[25]

[24] Harvard Business Review, 12 June 2018
[25] Statista.com

Security Concerns

A review of literature on potential problems associated with smart cities uncovers such words as "catastrophic" and "apocalyptic"—terms not typically used when describing urban planning or infrastructure design. But critics and even supporters are concerned by the possible damage that can be caused by attacks on networks supporting smart cities.

> Water and filtration systems, smart lighting, traffic controllers, utilities and more all become intertwined in smart cities, which aim to make urban living more energy efficient, eco-friendly and manageable. However, connecting all of these critical elements can have devastating effects should something go wrong—such as a successful cyberattack.[26]

Much of the concern focuses on infrastructures being connected through a single network, which offers benefits such as data accuracy and transmission speed, but also represents a clear path for infiltrating a city's entire network. The possible repercussions of such a breach can be potentially devastating. The difference between an attack on a business and on a city is the potential physical risks posed by malfunctioning critical infrastructures and the significantly greater scale in a city.[27]

The specific risk to smart cities involves hackers gaining access to a sensor, enabling them to more easily breach a city's network. They can target administrators' privileged accounts and access sensitive information and system controls. Another important consideration is internal threats, as cities must also ensure that employees are accessing only the systems and data they are authorized to view. Security experts have suggested the introduction of identity and access management (IAM) protections is necessary to provide essential protections for citywide systems.[28]

> Smart cities are "apocalyptic scenarios managed and mitigated by sensor-based solutions," reliance on which can lead to danger.
>
> **Rem Koolhaas**
> Dutch architect and professor[29]

Examples of Cyberattacks on Infrastructure

Perhaps the most severe cyberattack on a political entity occured in December 2015, when Ukraine suffered a massive cyberattack that led to an interruption of electricity and water supplies for 230,000 residents during an extremely cold winter.[30]

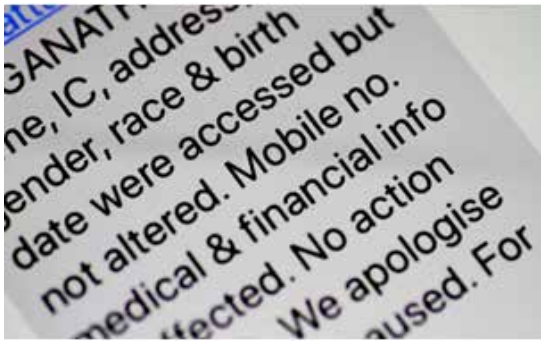
This attack, which was the first confirmed sabotage of a grid, was likely conducted by highly sophisticated attackers, with security researchers linking the incident to a Russian hacking group known as "Sandworm"[31] and possibly state actors (Ukraine's intelligence community claims Russia was behind the attack). Of note is that the control systems in Ukraine were more secure than some in the U.S., since they were well-segmented from the control center business networks with robust firewalls. However, a flaw with the Ukrainian system is that two-factor authentication was not required to log in to the network, which allowed the attackers to hijack workers' credentials and gain access to systems that controlled the breakers.[32]

[26] ZDNet , 9 August 2018
[27] Security Magazine, 27 January 2018
[28] One Identity, Building a smart city starts with security
[29] European Commission, Rem Koolhaas, 24 September 2014
[30] Security Magazine, 27 January 2018
[31] Reuters, 26 February 2016
[32] Wired, 3 March 2016

> "The people in charge of the world's power supplies have been warned. This attack was relatively short-lived and benign. The next one might not be."
>
> **Kim Zetter**
> Wired, 3 March 2016 [33]

While the attack against Ukraine was the most crippling, there was evidence of a widespread cyber attack on a nation's infrastructure as far back as 2007, when much of Estonia's internet was inaccessible for 24 hours and citizens could not access government websites, bank accounts or online newspapers. The source of the disruption was a Distributed Denial of Service attack (DDoS), which is a coordinated deluge of internet traffic, for example from ping floods and botnets, that overwhelms servers and shuts down websites. Like the Ukraine attack, several analysts suspect Russia was also behind the attack and Estonian President Toomas Hendrik Ilves said, "looking back on it, it was the first, but hardly the last, case in which a kind of cyber attack…was done in an overtly political manner."[34]

Examples of other attacks include the theft of 1.5 million patients' sensitive health data—including Prime Minister Lee Hsien Loong's records—in Singapore from 1 May 2015 to July 2018.[35] The stolen information included patients' name, national identification number, address, gender, race and date of birth, while raising concerns for Singapore's Smart Nation Initiative, which was started in 2014 to integrate various technologies such as medtech, fintech and govtech to create a digital smart city-state.[36] And DDoS attacks delayed trains and disrupted Sweden's transportation network causing operational delays in October 2017, while a similar attack prevented DSB, the largest train company in Denmark, from selling tickets to passengers in May 2018.[37]



An SMS message sent by SingHealth to clients affected by a cyberattack is seen on a mobile phone in Singapore
Source: Reuters, 23 July 2018

While not as widespread or severe as the Ukraine attack, **U.S. cities have also experienced attacks that impacted vital networks**. One example occurred in Atlanta, which was the target of a major ransomware attack in March 2018 that resulted in outages across the city's digital systems, while wiping digital records and forcing city officials to manually work with paper files in the weeks following the attack.[38]

Another example of an attack in the U.S. occurred a week later in Baltimore, where the city's 911 system was temporarily shut down after a ransomware attack. The Baltimore attack happened after a city information technology team troubleshooting a separate server issue inadvertently changed a firewall and left a port open for about 24 hours. Hackers who were likely running automated scans of networks looking for such vulnerabilities found it and gained access.[39] This attack was significant, but hardly

[33] Wired, 3 March 2016
[34] Foreign Policy, 27 April 2017
[35] ZDNet , 9 August 2018
[36] The Asean Post, 24 July 2018
[37] Transport Security World, 14 May 2018
[38] Smart Cities Dive, 26 July 2018
[39] The Baltimore Sun, 29 March 2018

unusual, as there were 184 disclosed cyberattacks on U.S. public safety organizations during 2017 and 2018, 42 of which were directed at 911 services.[40]

> "I don't know what else to call it but a self-inflicted wound. The bad guys did not get in on their own without the help of someone inadvertently leaving the door open."
>
> **Frank Johnson**
> Chief Information Officer, Baltimore Mayor's Office of Information Technology[41]

The San Francisco Municipal Transport Agency was also the victim of a malware attack that infected more than 2,000 computers in November 2016. Core operations were not impacted and train service was maintained, but email and payment services were disrupted. Revenue was impacted as city officials decided to open the gates so passengers could board trains without payment.[42]

Size and geographic region do not provide any additional protection for a city, as attacks have happened recently in such cities as Medford, OR, Wellington, FL, and Bozeman, MT. Data breaches from online billing systems followed attacks on the Click2Gov network that impacted the three cities.[43]

Security Preparations by Smart Cities

As municipalities ramp up smart city activities, some are preparing for the inevitable attacks on their networks by conducting tests to bolster their defenses. Houston, for example, ran a three day exercise in July 2018 to determine the city's readiness for repelling malicious threats. The test involved a simulated natural disaster and cyberattack happening simultaneously. Mayor Sylvester Turner said, "the exercise will allow us to examine the challenges those incidents place on critical infrastructure, while assessing response capability, agency collaboration, communication interoperability, and military integration." New York City had previously run a Jack Voltaic 2.0 test, which helps municipalities understand threats to vital services.[44]

The U.S. Army has partnered with local governments and private enterprises to help cities deter attacks against critical infrastructures. Col. Andrew O. Hall, director of the Army Cyber Institute, believes robust exercises are beneficial, because "gaps in cyber defense become apparent and leaders of these communities learn what actions they must take to defend themselves." The Army also benefits, as the lessons learned from "live fire" exercises help them better understand how to defend vital networks, which have implications for national security.[45]

Andrew Salkin, senior vice president for City Solutions at 100 Resilient Cities, said that cities need to think beyond "we're going to protect ourselves from attacks," and instead "think about the services that the city has that are connected to technology that can be enhanced, protected and leveraged to help the city do a lot of different things."[46]

Security Recommendations

Evidence indicates smart cities already have vulnerabilities that can potentially be exploited, as many devices, systems and technologies powering smart city features are still being developed without appropriate security architectures or threat mitigation solutions.[47] Researchers with IBM's X-Force Red and Austin-based cybersecurity company Threatcare found 17 new vulnerabilities with smart city systems used across the world, including entire city systems that can be accessed

[40] RFID Journal, 20 January 2019
[41] The Baltimore Sun, 29 March 2018
[42] The Gaurdian, 28 November 2018
[43] Smart Cities Dive, 26 July 2018
[44] Houston Public Media, 25 July 2018
[45] Army News Service, 26 December 2017
[46] Smart Cities Dive, 26 July 2018
[47] Smart Cities World, 23 January 2019

due to such common security issues and 'old school' threats as **default passwords and networks exposed online that are easy to find**. "These are devices that can be exploited without any type of prior knowledge," according to Daniel Crowley, a research director with IBM's X-Force Red. "These are Application Security 101 types of issues. You shouldn't be exposing any devices to the entire internet."[48]

To address potential vulnerabilities, the Threatcare and IBM X-Force Red researchers believe the following mediation techniques can be helpful:

- First, implement IP address restrictions to connect to the smart city systems
- Second, leverage basic application scanning tools that can help identify simple flaws
- Safer password and API key practices are obviously necessary
- Security incident and event management (SIEM) tools will also help to identify suspicious traffic. But someone needs to be observing what is going on in the first place. The research dramatically shows the means by which interconnected cities can be manipulated by attackers. A frontline defense has to be established by those who are using the technology.[49]

Other recommendations come from a report[50] released in February 2019 by the New America think tank, which suggests cities across the U.S. (and probably worldwide) should **hold regular cyber exercises and have incident response plans to cyberattacks**, as many municipalities may not have sufficient protections for such incidents. "No amount of repetition would be excessive to hammer home the point that exercises are key to maximizing efficiency and effectiveness of incident response capability and resources," Natasha Cohen, a cybersecurity policy fellow at New America, stated in the report. Cities should also form partnerships with other governments in the same area or region to share resources, according to the report.[51]

In an interview with *WSJ Pro Cybersecurity*, Ms. Cohen noted San Diego's Chief Information Security Officer (CISO) meets with CISOs from local businesses to exchange information. "They have been able to share very tactical information about attacks that are hitting the area and it's an idea that is really taking off. Building that trust can be done much better in a regional mode. It has a lot to do with the ability to meet face-to-face [and] connect based on what's going on in your community." She also said "sharing a CISO is something we're suggesting they might be able to do either through a state-run program where they hire someone and they do chargebacks for the person's time or having one city hire the person and doing chargebacks city to city."[52]

There are few established standards or regulations for cities developing smart technologies, however, so approaches to security may vary and even appear to be haphazard. Factors such as the competence and experience of a city's CISO, as well as a city's resources and how those funds are allotted will affect a municipality's readiness to protect the systems that enable smart cities, with broad disparities in preparedness the likely result. **The sharing of best practices or development of collaborations and associations will be helpful,** but greater uniformity and the establishment of protocols for security may not occur before higher profile breaches occur.

[48] CNET, 10 August 2018
[49] Security Now, 10 August 2018
[50] Cyber Incident Response and Resiliency in Cities, New America, February 2019
[51] Washington Post: The Cybersecurity 202, 22 February 2018
[52] WSJ Pro Cybersecurity, 25 February 2019

WSJ PRO CYBERSECURITY
Smart Cities: Technological Wonders or Security and Privacy Threats?

Do Smart Cities Compromise Privacy?

> "As with other forms of social media analytics, the potential to mine the data for more personalized information and targeting of city services are endless and hence, there is a continuous risk of these services being pulled towards the more problematic quadrant where privacy is at stake, and purpose may shift away from service to surveillance."
>
> Erasmus University of Rotterdam study about privacy concerns in smart cities[53]

Smart cities need to collect massive volumes of data to determine patterns and behavior that enable infrastructure to function at peak efficiency. This creates a possible tension between the use of data for the public good and surveillance, as privacy experts have raised concerns about how data collected on individuals may be used without their knowledge or consent.

The U.S. Federal Trade Commission's (FTC) "Privacy & Security in a Connected World"[54] report revealed that fewer than 10,000 households can generate 150 million discrete data points every day. The security risk this creates is apparent, as more entry points and sensitive information becomes available for cyberattackers.

From a privacy standpoint, this massive volume of data creates a risk that companies harvesting information might sell the data for marketing purposes. Consider the case of Facebook selling personal information about millions of users to political research firm Cambridge Analytica without the knowledge or consent of those users. The FTC report also noted a possibly overlooked risk is that more IoT products are sold for a lower price than non IoT products because the user is more valuable from a data standpoint than the devices.

Privacy matters can also lead to security concerns. An April 2019 Bloomberg article revealed that an Amazon team responsible for auditing Alexa to improve its performance could access users' location data and, in some cases, learn a user's home address. "Anytime someone is collecting where you are, that means it could go to someone else who could find you when you don't want to be found," according to Lindsey Barrett, a staff attorney and teaching fellow at Georgetown Law's Communications and Technology Clinic.[55]

Toronto's Privacy Controversy

Perhaps the most high-profile example of smart city privacy concerns to date has taken place in Toronto, where Google parent Alphabet has been working on transforming Toronto's eastern waterfront into a smart city, with the goal of making the neighborhood more affordable and sustainable. However, the project has received criticism from locals and privacy advocates who are worried about how Google-affiliated Sidewalk Labs will use the data it collects from the project.

Sidewalk Labs has claimed it will not control the collected data, but that assertion was not enough to prevent the Director of Privacy for Sidewalk Labs, Ann Cavoukian, from resigning from the project. Ms. Cavoukian, the former privacy commissioner for the province of Ontario, left because she learned not all data collected from residents would be anonymized at the source and compared the project to a "smart city of surveillance."[56] Sidewalk Labs has countered by

[53] GovTech.com, 26 February 2018
[54] Internet of Things: Privacy & Security in a Connected World, Federal Trade Commission, January 2015
[55] Bloomberg, 24 April 2019
[56] Forbes, 8 January 2019

claiming it should not formulate rules for third parties on its own and has proposed creating a "Civic Data Trust" to develop that policy.[57]

The resolution of this and similar privacy situations are important as there are burgeoning public-private partnerships between city governments and technology companies due to smart city growth. Municipalities have begun partnering with such companies as IBM, Cisco, Nokia and Huawei, who have introduced their platforms and in some cases are providing end-to-end solutions.[58]

San Francisco Bans Facial-Recognition Surveillance

San Francisco became the first U.S. city to ban the use of facial recognition by local agencies after the Board of Supervisors voted overwhelmingly (8-1) for the ban on May 14, 2019. The provision, which also requires city agencies that want to purchase a surveillance system to first receive approval from the board, was largely a response to critics of the technology who believe it can perpetuate police bias and provide excessive surveillance powers for authorities. The ban runs counter to a recent trend that has seen dozens of police departments use facial recognition technology to review databases with mug shots and driver's-license photos to identify suspects.[59]

> "There must be an appropriate balance between those who subscribe to Orwell's Big Brother mentality and those who want to prevent car break-ins and porch-package thieves."
>
> **Tony Montoya**
> President of the San Francisco Police Officers Association[60]

Privacy vs. Convenience: Conflicting Messages From Respondents

> "We as a country—and even the world over—are far too interested in doing things faster, smarter, and more easily that I do believe we will continue to offer our data up to companies working to improve our lives through connectivity."
>
> **Daniel Newman**
> CEO of Broadsuite Media Group[61]

Privacy issues are legitimate concerns raised by experts and consumers alike. But in the age of social media, with more of peoples' lives willingly exposed than ever before and a company such as Facebook increasing users in Q1 2019 despite widely reported incidents of using data without users' permission, it seems unlikely many smart city projects will get derailed over privacy concerns. **One study found 60% of citizens would likely approve a ballot initiative involving smart city activities in their community.**[62] Daniel Newman of Broadsuite Media Group said it will be interesting to witness the reaction to the initial smart city breaches, but he believes the influx of targeted messages and ads will not deter smart city development and the speed and convenience offered by connected lives.[63]

Supporting the seemingly contradictory notion that consumers are concerned about privacy and yet may not take appropriate action are the results from a February 2019 survey by IBM's Institute for Business Value. On the one hand, 81% of consumers say they've become more concerned about how companies use their data, while 87% think companies should be more heavily regulated on personal data management. Additionally, 75% of respondents said they were less

[57] MIT Technology Review, 24 October 2018
[58] Computer Weekly, July 2018
[59] Wall Street Journal, 14 May 2019
[60] Ibid
[61] Forbes, 8 January 2019
[62] The Hill, 9 October 2017
[63] Forbes, 8 January 2019

likely to trust companies with data and 89% said companies should be clearer about how their products use data. Despite these concerns, 71% of respondents said that they were willing to give up privacy to get access to what technology can offer, while just 45% claimed they have updated privacy settings and only 16% stopped doing business with an entity due to data misuse.[64]

> "Yes, privacy is a concern, but convenience is king — as too is cost savings. So for many consumers, the promise of enhanced conveniences and reduction in household costs — i.e., connected thermostats, lights [that] can reduce energy consumption — is a big overriding factor that explains why consumers continue to purchase and use these devices despite the privacy risks."
>
> **Adam Wright**
> Senior analyst at market intelligence firm IDC[65]

Data Contracts

According to Carlo Ratti, director of the Massachusetts Institute of Technology (MIT) Senseable City Lab, the best approach for preventing potential misuse of data is for smart city governments to implement a "data contract" between individuals, companies, and governments.

An example of this type of contract comes from the General Data Protection Regulation (GDPR), which requires all businesses within the European Union to reveal what kind of data they collect from EU residents and to receive individuals' consent for its use (though it does not address data collection by governments). Under the law, EU citizens also have the right to opt out and have personal data removed from any database if they believe there is no longer a compelling reason to keep it.[66]

Citizens' Right to Anonymity

A survey conducted by McMaster University found that 88% of Canadians are concerned about their privacy in smart cities, with 23% of the respondents being extremely concerned. The leader of Ottawa's Smart City 2.0 initiative, Marc René de Cotret, says privacy in the next generation of smart city technology is something to be taken very seriously. The city's fundamental principle is that every citizen "needs to have full control of their data. If you want to stay anonymous, you should be able to do that." To support this premise of citizen control, Ottawa is testing an app in spring 2019 that is designed to send alerts to residents about parking bans and garbage collection updates, with users having the option of blocking the GPS tracking function.[67]

Implications of 5G Networks?

> "5G implies faster speeds for good guys and for bad guys."
>
> **Galina Datskovsky**
> CEO of secure messaging company Vaporstream[68]

Perhaps the most anticipated technological innovation of 2019 has been the introduction of 5G networks, which are expected to bring faster phones, smarter tech and more seamless services. While 5G networks may be pivotal to the development of smart cities and associated services such as autonomous cars and improved health care, several observers warn that privacy and security concerns also need to be addressed. Marc Rotenberg, president of the nonprofit Electronic Privacy Information Center, notes that with the expected exponential growth of network-connected 5G devices, "governments will need to test

[64] Axios, 25 February 2019
[65] Vox, 13 May 2019
[66] Futurism, 7 November 2017
[67] Ottawa Business Journal, 19 March 2019
[68] USA Today, 28 March 2019

these systems carefully before they are deployed and end-to-end encryption for network traffic should be a priority."[69]

Sasa Radomirovic, an information security specialist at the University of Dundee, explains that "for each 5G equipped thing, there will be the possibility that an attacker or manufacturer abuses it to invade your privacy." For example, Chinese telecommunications giant Huawei has been accused by officials in a number of governments of possibly installing 5G network equipment that could be used for espionage activities. The introduction of 5G networks, Mr. Radomirovic and other analysts note, is a risk that must be balanced with improved connectivity to enhance various services.[70]

> "5G is not just for refrigerators. It's farm implements, it's airplanes, it's all kinds of different things that can actually kill people or that allow someone to reach into the network and direct those things to do what they want them to do. It's a completely different threat that we've never experienced before."
>
> **Robert Spalding**
> Senior fellow at the Hudson Institute and former senior director for strategic planning at the National Security Council[71]

Preparations and Recommendations for Security and Privacy in Smart Cities

Much like the collaborations being developed to assist municipalities with preparing for the emerging security threats involving smart cities, **associations are being developed to assist officials with navigating the intricacies of emerging privacy issues**, as well as sharing best practices and promoting fair and transparent data practices. The Civic Data Privacy Network was introduced in March 2019 to help city leaders by sharing practical guidance, with government officials from municipalities such as Seattle, Portland, Washington, D.C., and Oakland joining the new network.[72] The following mission statement was developed by the network to advance civic data privacy:

- Create a comprehensive Privacy Risk Assessment for smart and connected community projects, providing guidance to local governments and technology providers and ensuring projects serve the common good.
- Expand the network of privacy leaders for smart cities and creating peer networks, best practices, and practical tools for responsible data use.
- Host workshops in conjunction with MetroLab Network, the South Big Data Innovation Hub and others in order to share best practices and identify areas for further research and collaboration.

> "It can be tough to have a technical debate with engineers from Google who come in with really fancy software and they talk about how thoughtful they've been with anonymization and it requires pretty advanced understanding of the topic to be able to see the flaws and push back on that type of thing."
>
> **Ben Green**
> Former Data Scientist in Boston's Department of Innovation and Technology[73]

[69] USA Today, 28 March 2019
[70] Ibid
[71] The New Yorker, 26 April 2019
[72] Future of Privacy Forum, 28 March 2019
[73] Red Tail, 14 April 2019

Conclusion

Smart Cities offer a glimpse of the future, yet several of their key components already impact our lives, with many of us taking advantage of their services on a daily basis, whether or not we are aware of them. Driving on streets monitored by traffic sensors, working in a building that turns off the lights after the last employee leaves and emergency services prepared to assist citizens in times of need are all smart functions that are part of the networks that will be commonplace not only in cities, but eventually towns and villages.

But like so many innovations, the conveniences of smart city technologies come with a cost: risks to security and possible intrusions into private lives. Experts and interested observers alike have expressed concern about the disruptions cyberattacks could cause to networks and grids that provide vital services, with a growing list of such events that have already occurred. Awareness of these liabilities are rising among the citizenry, with city planners and government officials hearing their concerns.

Both risks are preventable: Security attacks can be blunted through a well-trained workforce that follows proper security protocols, while public officials can listen to their constituents' concerns and ensure the proper privacy standards and regulations are in place, including options for individuals to remain anonymous and opt out of sharing certain data. Of course, these protections may run smoothly in a perfect world, but exceptions will certainly happen in the real world. Defenders will inevitably let down their guard or accidentally leave openings in networks so attackers can penetrate their systems, while the potential for insiders to abuse their privileges and violate the reams of data available to them is significant.

Do the risks outweigh the benefits of smart cities? Surveys show that most individuals are more interested in the benefits and conveniences offered by smart cities than the risks associated with them. Accordingly, the development and growth of smart cities are inevitable, so businesses would be wise to prepare how they will operate in smart cities or even contribute to their development. And the already high demand for cybersecurity professionals and services will only increase, along with the need for privacy officers to monitor the activities of privileged officials and workers within smart cities.

> "Smart Cities 1.0 saw significant advances in connected technologies. Smart Cities 2.0 will be a public policy response to 1.0. The Internet of Things, autonomous systems, and 5G have clear consumer, enterprise, and national security implications. The policy decisions on Smart Cities 2.0 will either accelerate or stifle urban innovation. The consequences are enormous."
>
> **Brendan Hart**
> Director of Global Cities at the University of Virginia's National Security Policy Center
> Host of the Super Cities podcast[74]

[74] Interview with WSJ Pro Cybersecurity

Meet the Authors

DAVID BREG is senior research manager at WSJ Pro, focused on providing actionable intelligence for readers interested in learning about issues involving cybersecurity through white papers and other research activities. Dave has been at Dow Jones for 12 years, supporting customers in various analytical and advisory roles on a range of topics that includes artificial intelligence and information security. Dave has prior experience managing the research unit at public relations firm Burson-Marsteller and policy knowledge from serving as an advisor to a Member of Congress and as an analyst at the Congressional Research Service.

Write to Dave at **david.breg@dowjones.com**

ROB SLOAN is research director at WSJ Pro focusing on providing thought leadership, building datasets, and contributing to the WSJ Pro Cybersecurity newsletter. Previously, Rob was response director for a specialist IT security consultancy in London and built a team focused on detecting, investigating and protecting against cyber intrusions and responding to incidents, especially state-sponsored attacks. Rob started his career working for the U.K. government, looking at some of the earliest cyberattacks against the critical national infrastructure. Rob's main interest is the requirements, motivations and technical capabilities of threat actors to understand the attacks in the context of the intelligence of the states carrying them out.

Write to Rob at **rob.sloan@dowjones.com**

DOW JONES

WSJ PRO CYBERSECURITY

Smart Cities: Technological Wonders or Security and Privacy Threats?

WSJ PRO CYBERSECURITY

Managing Cyberrisk for Executive Travelers

Introduction

Most large organizations have implemented programs that have transformed the way they manage and counter cyberrisk. However, even with expanded teams of skilled cybersecurity professionals, an explosion of vendors providing solutions to every possible risk, and maturing processes, there are still areas where enterprises fall short and leave data vulnerable.

One such area is around how companies coach staff to make the right cybersecurity decisions. In the office that means not opening files from unknown senders or browsing to untrusted websites, but what about when the employee leaves the office? How do we prepare an employee for the risks they may face thousands of miles from home? In most cases, relatively simple measures can be implemented to have a positive impact without overly inconveniencing employees trying to do their job.

My colleague, Marilia Wyatt, and I have compiled this report containing all the advice organizations need to understand, manage and mitigate travel risk. Additionally, we set out the content of a travel risk roadmap. While the focus is the executive traveler, much of the advice is generic to all employees.

We welcome your feedback.

Rob Sloan
Research Director, WSJ Pro
rob.sloan@dowjones.com

Executive Summary

Corporate travel overseas brings a number of cyberrisks that are not typically concerns for executives based in North America or Western Europe. The risk of corporate and personal devices being targeted by foreign officials for the information stored on them increases with travel. Businesses must carefully consider how lost or stolen devices could put corporate data at risk.

Providing executives with an awareness of business travel cyberrisks and writing policy for all staff with simple mitigating controls can significantly reduce the likelihood of significant impact arising from the loss, theft or compromise of a device while overseas.

There is no one-size-fits-all approach. While much of the advice in this document is relevant for all organizations and their staff, some measures will vary on a case-by-case basis. Enterprise risk officers must implement appropriate controls for their organization and, where necessary, tailor these to individuals, or types of traveler to ensure the right balance between security and convenience. If that balance is wrong, the policy will be ignored, not least by senior executives who set the 'tone at the top'.

Implementing recommendations made in this report will require coordination across the business including, but not limited to, stakeholders working in cybersecurity, privacy, risk and compliance, physical security, technology, human resources, legal, and communications.

Key Takeaways:

- Organizations must assemble a cross-functional team to assess the risk to corporate data from overseas travel and to understand what data and resources employees, particularly senior executives, require while traveling.
- A cybersecurity travel policy is required to ensure travelers know what is expected of them to minimize the risk of corporate devices, and the data residing on them, being lost, stolen or compromised.

> *In most cases, relatively simple measures can be implemented to have a positive impact without overly inconveniencing employees trying to do their job.*

Background

Video-conferencing and virtual-meeting solutions have done little to stem business travel. Meeting remote customers and partners, attending and participating in trade shows and conferences, visiting overseas offices and facilities, and business development all still require individuals of all levels of seniority to travel abroad on behalf of their organization.

Despite the obvious risks to corporate data while away from an office location, few organizations have well-developed policies designed to protect business travelers as they move around the world. While the loss or theft of a corporate laptop or smartphone is the most likely incident travelers may face, there is always a risk that foreign government officials could target travelers to gain access to data stored on devices or to compromise a device for exploitation later.

The loss or theft of a device can cost far more than the replacement value of the hardware. Some reports have put the cost at over $49,000*, which includes the expense of breach notifications, lost productivity, legal and potential regulatory costs and, in some cases, the loss of intellectual property on the device. When criminals or foreign government officials target travelers and devices, the cost can be much higher and far harder to calculate.

One reason policies are often ignored is because they are too prescriptive and do not balance security and convenience. Not every overseas business trip requires the same level of security: what is appropriate for one destination or job role may not be suitable for others.

Risks must be assessed and mitigations applied appropriately. In general, senior executives and government officials face a higher level of risk, especially when traveling to a hostile country. The threats and risks faced by one organization may be very different from those faced by another, even within the same industry. If policies are deemed draconian or the risks are over-stated, they will be ignored.

The purpose of incorporating and managing cybersecurity travel best practices proactively into a travel risk program is to operationalize cyberrisk management frameworks and processes to enable risk officers and relevant stakeholders to identify, measure, prioritize, and mitigate travel cyberrisks in their organizations.

The ultimate goal of any program is to strengthen cybersecurity resiliency through improved risk identification and management, and enhanced programs for employee cybersecurity awareness and action.

This report provides executives and risk officers considerations to incorporate cyberrisk mitigation controls into corporate travel risk programs, and necessary awareness of most common cyberrisks travelers encounter and example countermeasures.

*Ponemon Institute: The Cost of a Lost Laptop, 2009

Key Travel Risks & Advice

The controls each organization decides to implement will vary extensively. There is no one-size-fits-all policy. The guidance below is intended to be useful for all organizations, though discussion and tailoring of the solutions is required.

Pre-Travel Guidance

- Employees intending to travel to countries deemed 'higher risk' by the organization must first seek advice from the organization's security or risk officer. Controls will vary according to the employee's role, the purpose of their trip, the data they will be carrying and the reason the destination has been assessed as 'higher risk.'
- A cyberrisk briefing, tailored for key employees or high-risk destinations, will deliver risk awareness education and agree the controls to ensure the traveler's data remains secure. Employees will be provided with advice to appropriately secure 'non-clean' devices.
- Clean-build devices (including laptops and smartphones) must be available at short notice and with minimal fuss for the traveler. This process must focus on the requirements of the traveler to ensure they can function without hindrance. Any significant inconvenience could lead to controls being bypassed.

What is a 'Clean' Device?

To minimize data loss if a device is lost, stolen or compromised, many organizations stipulate that employees must take a 'clean' device to high-risk destinations. A clean device is a laptop, tablet or smartphone that provides access to company resources critical for the traveler – such as email – but does not contain documents and data created or stored by the user, or data associated with the user such as saved passwords, cookies and browsing history.

A clean device may not even require a connection to the corporate network. Data required by the traveler is loaded onto the device pre-travel and data created during the trip is transferred back to the user post-travel.

To prepare the device for the next trip, it is thoroughly wiped, and the operating system is re-installed.

Case Study: Smartphones at Risk

Mobile devices are susceptible to attacks and physical access to devices left behind in hotel rooms or examined at airport security makes life easier for attackers.

In early 2018, mobile security company Lookout, Inc, and the Electronic Frontier Foundation reported on research that highlighted attacks against military personnel, enterprises, medical professionals, activists, journalists, lawyers, and educational institutions. The attacks were attributed to the Lebanese government highlighting the intent and capability found even in developing nations.

Mobile users were tricked into downloading malicious copies of legitimate applications such as WhatsApp and Signal. These applications had extended permissions that gave attackers access to all stored data and even exploited the microphone to allow eavesdropping on the device's environment.

Guidance During Travel

- If the traveler has suspicions of a machine having been tampered with, they should make detailed notes about dates/times, circumstances and any unusual machine activity. This will aid investigators later. Ideally, the machine will be switched off until such time as it can be thoroughly examined.
- The traveler should not leave laptops or mobile devices unattended at any point. Physical access provides attackers with multiple options to compromise devices.
- Internet connectivity is required during travel, but public WiFi hotspots should be avoided wherever possible. Travelers should be reminded that if hotel WiFi use cannot be avoided, use of a corporate Virtual Private Network (VPN) to keep communications secure is essential. A mobile phone hotspot offers more security than untrusted WiFi connections.

Case Study: Hotel WiFi Users Targeted

Several cybersecurity companies have reported on attacks attributed to the North Korean state that targeted executives staying at luxury hotels across Asia. Evidence shows the group carrying out the attacks was active since at least 2007.

Once connected to the hotel's WiFi network, users were instructed to perform a software update that compromised their laptop. The attackers used software exploits for which no security patches were available. Data was subsequently stolen from the infected machine. It is not clear how the stolen data was used.

Overseas Communication Risks

No telephone conversation, mobile or fixed line is ever secure. The telecoms company providing the roaming service will have full access to voice calls, text messages, internet browsing data, location data (from cell site analysis, not GPS) and numbers of remote parties. In most countries, the government will share the same access.

Local SIM cards do not represent a more secure option than using a regular SIM card in roaming mode. Local payphones are equally susceptible to eavesdropping, and your use of them may draw attention and be seen as suspicious. Governments may monitor IP communications.

Organizations may wish to consider encrypted calling or messaging while considering whether that would break local laws or unnecessarily draw attention to the user.

Post-Travel Guidance

- The traveler should report any incidents immediately upon return from travel with contemporaneous notes detailing suspicions if they were not communicated during the trip.
- Data created and stored on loan devices should be first scanned for malware by cybersecurity staff, then transferred back to the traveler. Loan devices should then be wiped and rebuilt for future deployment.
- Where incidents have been noted or investigated, details must be added to a corporate security 'memory' to ensure they are retrievable in the future by anyone in the risk or security team.

Observe Good Cybersecurity Hygiene:

Hygiene measures do not guarantee security, but they can significantly reduce the risk of compromise. These are the equivalent of being told to wash your hands properly – it doesn't guarantee that you won't catch a cold, but it certainly helps in minimizing germs. Follow these tips to improve your digital hygiene.

- Protect all devices and accounts with strong passwords.
- Backup device data regularly according to your organization's policy.
- Be vigilant about social engineering attempts aimed at getting you to open attachments, click on links, download applications or interact with social media.
- Enable two-factor authentication on all personal and work accounts where possible.
- Ensure all software is up-to-date and security patches are installed.
- Turn off WiFi, Bluetooth and location services when not in use.
- Avoid connecting to unsecured or untrusted WiFi hotspots.
- Use encryption to protect data in transit and stored on your devices and for communications.

Cybersecurity Travel Risk Program Roadmap

Creating a reliable cybersecurity travel risk program or strategy should begin with a roadmap and this section outlines the basic steps. The aim of the roadmap is for risk officers to create a program that shifts from reactive measures to a proactive and strategic mechanism to identify and manage travel cyberrisk in their organizations.

1. Identify Cross-Functional Internal Stakeholders

- Stakeholders from cybersecurity, physical security, legal, human resources, business continuity, and a senior executive sponsor must bring their expertise to the initiative to identify the scope, aim and objectives of the project.

2. Identify Low, Medium and High-Risk Destinations and Design Corresponding Cybersecurity Controls

- Understand executives' specific travel needs, especially those who travel frequently or travel to high-risk locations.
- Controls must be designed with minimal disruption for the traveler. Employees want to do their jobs and overly prescriptive controls will be ignored.
- Understanding the reasons behind travel and the technology and applications employees, especially executives, rely on while traveling will help with the control design. Employees will typically always need access to emails, but may not need to access sensitive databases or applications.
- Some controls may actually favor the traveler. Employees may be willing to swap their heavy corporate laptop for a lightweight tablet which provides access to internet, email and office functionality, but which does not contain sensitive company data or provide access to applications.

3. Use Booking Process to Identify Travel to High-Risk Countries

- Identifying employees traveling to high or medium-risk destinations should not rely on self-reporting. Can the travel booking process be leveraged to alert security staff to individuals planning trips to high-risk locations?
- Can travelers to low-risk countries be provided with risk mitigation tips via email as part of the booking confirmation workflow?
- Analyzing historical travel data will provide the security team with data on the frequency of travel to each destination and the roles of those traveling to scope the expected workload associated with a new program. Consider how the use of this data may be covered under global and U.S. federal and state privacy laws and seek input from privacy team to identify and mitigate potential privacy risk.

4. Create a Travel Cyberrisk Policy to Detail Exactly What is Expected of Employees

- Only by committing the rules to policy will employees fully understand how seriously the organization takes travel cyberrisk.
- Stakeholders can decide whether disciplinary action will be taken against employees who willfully ignore the policy and put corporate data at risk.
- Create an advice channel where employees can get guidance before, during or after their trip. The channel should be monitored at least within office hours and include a function for simple, encrypted communications.

5. Create Executive Travel Cyberrisk Briefing and Debriefing Process

- A policy alone is not enough to ensure the security controls are followed. The policy must be socialized with accompanying awareness materials to explain why it is important and in which circumstances employees should seek guidance.

- Awareness briefings must be ongoing to guarantee employees remember to consult the risk officer ahead of higher-risk travel. The process for doing this must be frictionless for the employee. Wherever possible, details of real incidents faced by staff, sanitized where necessary, should be circulated to reinforce the fact the risk is real.

- Routine traveler debriefs are an important part of the process.
    - Employees returning from low-risk destinations can receive a post-travel email reminding them to report any issues.
    - Employees returning from medium-risk destinations should receive a phone call asking whether they had any issues.
    - Employees returning from high-risk destinations should have a face-to-face debrief to discuss the trip.

- In addition to soliciting details of incidents, travelers should be prompted to provide suggestions for program improvements. This is key to making the program relevant. Employees may have suspicions they would not report unless prompted to do so.

6. Audit to Keep Program Alive and Relevant

- Each business trip presents risks and opportunities, making auditing and evolving the policy and program fundamental to its success.

- The audit should aim to identify gaps in organizational support across business units as well as track incidents, policy breaches, trips to higher risk destinations and numbers of briefings/debriefings delivered.

- Over time the audit function will show whether the program has delivered the security and cost-savings expected.

Common Risks & Mitigations

Risk
Interception of communications.

Description
An attacker may be able to access an individual's communications, including email, messaging apps, and phone calls.

Probability
Low

This capability is beyond all but state-level attackers and the most sophisticated criminals. Few executives will be singled out for surveillance unless the intelligence gain will be significant.

Impact
High

The attacker will have access to communications that may provide them with a strategic advantage. Alternatively, the information can be used to carry out a social engineering attack for persistent access to devices.

Control
Secure devices, communications, and internet use with encryption to ensure contents and communications are not susceptible to eavesdropping by third-parties.

Action
Brief executives on using Virtual Private Networks (VPNs) use to secure public WiFi connections. Advise staff to keep phone and internet communications to a minimum while in high-risk locations. Consider the use of encrypted messaging and calls apps. Remind employees on the risk of installing untrusted apps to their smartphones.

Risk
Unauthorized access to corporate devices.

Description
Airport security officials may inspect or even tamper with devices in order to view data stored on the device.

Probability
Medium

All travelers are subject to searches and airports provide law enforcement and intelligence officials an easy environment to conduct operations. Access may or may not be targeted.

Impact
Medium

An official simply viewing data is unlikely to have serious impact. However, physical access leading to the compromise of the device or a hard drive being copied could result in a significant data loss and longer-term impact.

Control
Provide travelers with clean devices that have no corporate network access.

Action
Travelers should be made aware of their obligation to comply with the demands of foreign officials, including (where necessary) providing access to devices. Wherever possible, passwords should not be shared and the traveler should not allow the un- locked device to be taken out of their sight, though they may have little choice in this regard.

Risk
Loss or theft of a corporate device.

Description
An employee may lose a device or removable media containing company data or a device might be stolen.

Probability
High

Devices are often lost during travel and thieves target business travelers all over the world because of the value of the devices they carry and the low likelihood of being caught.

Impact
Low

In the vast majority of cases, lost or stolen devices will be reformatted and sold. If the device is not encrypted there is the possibility data could be accessed. The targeted theft of devices is rare unless the target is of high-value.

Control
During mobile and laptop deployment, mandate full-disk encryption and remote wiping functionality after a maximum number of password entries. Consider banning the use of removable media.

Action
Provide briefing on security awareness education to avoid storing valuable data on removable media that could be easily lost or stolen. Understand data transfer requirements of users and find secure solutions. Consider providing staff with physical security awareness briefings to minimize likelihood of being the victim of crime.

Risk
Compromise of a corporate device.

Description
A device is targeted by an attacker to gain access to stored data or to provide ongoing access to the device.

Probability
Medium

Attacks may or may not be targeted. Officials may seek to compromise a high-value target device while the user is passing through airport security or has left the device unattended in a hotel room.

Impact
High

If an attacker has remote access to a company device it is likely there will be financial. operational, regulatory or reputational impact. The impact of the compromise will be felt beyond the single compromised device.

Control
Provide clean devices (laptops, mobile phones, and tablets) for high-risk travel and promote cyber-hygine measures. Limit privileged access to data and applications during travel, disable external ports and never leave devices unattended..

Action
Map out incident response plans that define role and responsibilities after a compromise. The plans should outline the processes to limit the damage and reduce recovery time and costs. Brief employees on preserving the device intact for forensic investigation when they return from travel. Remind staff that hotel safes are not secure!

General Cyberrisk Mitigation Guidance for Travelers

1. Understand Your Value as a Target

Executives regularly travel with data that could severely impact the organization if lost or compromised. Examples include personally identifiable information, intellectual property, commercial, strategic, financial, and medical data, research and development data, and negotiating positions. Assess the value, sensitivity, and criticality of data stored on your devices in the context of the purpose of the trip and understand how an attacker could leverage that data for personal, financial, commercial or strategic gain.

2. Use Encryption to Protect Data and Communications

A Virtual Private Network (VPN) encrypts all internet traffic and provides a level of assurance that no third-parties can eavesdrop on communication. Full-disk encryption will secure the data stored on the device if it is stolen. These simple measures provide privacy and security while working or traveling overseas. There is a wide variety of applications for smartphones that offer end-to-end encrypted messaging and call functionality.

3. Configure Automatic Wiping Settings and Create Strong Passwords

All devices should have a strong password to protect them and accounts from unauthorized access. Configuring automatic wiping settings can erase all data on devices (smartphones, laptops, tablets) after a predetermined number of passcode entry failures, which protects against unauthorized parties trying to access a device by guessing the password.

4. Bring Power Adapters and Cords

Avoid third-party charging station/devices where possible. Attackers can install malware on public charging kiosks to infect your devices or copy data. If a public charging station must be used, turn off your device before connecting to the power. Where possible, charge your phone directly from a main outlet rather than a USB outlet.

5. Airport Inspections of Devices are Common

Many countries give border officials authority to search laptops, smartphones or other digital devices. Travelers can face stiff penalties for failing to comply. Try not to let devices be taken out of sight or allow anything to be installed. If anything is plugged into a device or it is taken out of sight, assume it has been tampered with and try to avoid any further use of the device. Contact your cybersecurity team for advice.

6. Keep Devices Secure During Transit

To reduce the risk of loss, theft or compromise, secure devices while in taxis, at airports, on airplanes, events, and in your hotel room. Turning on 'Find My Phone' or similar device functionality can help locate a misplaced or stolen phone and organizations may provide similar software for laptops.

7. Avoid Using Removable Media

Removable media such as memory sticks or USB drives can store large quantities of data and are easily lost. They can also be infected to compromise devices they are plugged into. Do not accept gifts or promotional material on removable media.

8. Securely Connect to Internet

Wireless access points in hotels or coffee shops should be avoided due to potential risk of communications being monitored or the connection being exploited to compromise a device. Wired connections do not offer significant benefits over wireless connections. One solution to securely connect to the internet is to use a mobile hotspot via the phone's data connection.

Public computers in cafes and hotel business centers can have malicious software installed that monitors user activity and collects passwords and other data. Such computers are fine for general browsing – looking at maps, news, tourist info, etc., but not for accessing email, banking sites or accessing other personal / sensitive data.

Internet access is restricted in some countries. Be respectful of the culture of the destination country. Some websites or applications may be blocked and others may bring you to the attention of local officials. Attempting to bypass local restrictions on internet usage may be illegal.

9. Have Your Devices Inspected for Malware

The cybersecurity department can scan your devices and any external media for malware to minimize risk of malicious programs surreptitiously compromising the corporate network. If there is any suspicion that a device was tampered, do not connect to the corporate network until after it has been tested for malware.

10. Know Your Cybersecurity Unit's Contact Information

Keep contact details for the cybersecurity team in case of emergency. Writing down details about any incidents is beneficial for conducting forensic device investigations.

Government departments publish advice and guidance to travelers and help communicate the risk of travel to countries around the world. This is a useful resource when planning overseas travel.

Readers in the U.S. may wish to read the Travel Advisories on https://travel.state.gov before planning a trip.

Meet the Authors

ROB SLOAN is research director at WSJ Pro focusing on providing thought leadership, building datasets, and contributing to the WSJ Pro Cybersecurity newsletter. Previously, Rob was response director for a specialist IT security consultancy in London and built a team focused on detecting, investigating and protecting against cyber intrusions and responding to incidents, especially state-sponsored attacks. Rob started his career working for the U.K. government, looking at some of the earliest cyberattacks against the critical national infrastructure. Rob's main interest is the requirements, motivations and technical capabilities of threat actors to understand the attacks in the context of the intelligence of the states carrying them out.

Write to Rob at *rob.sloan@dowjones.com*

MARILIA WYATT is cyberrisk analyst at WSJ Pro. Marilia provides risk research and analysis, strategy, threat intel, and develops tools to augment and focus executive decision-making. Ms. Wyatt also serves on the Dow Jones Privacy Champion Council, where she advises internal stakeholders on proactive cyberrisk management and data privacy risk mitigation. Marilia founded and contributes to blog CyberPrivacy and manages the campaign #HackersforChange.

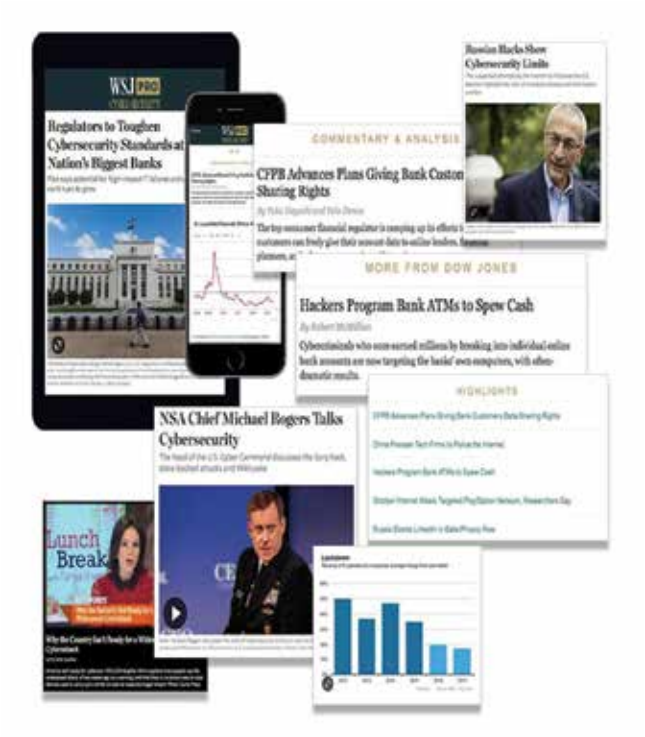
Write to Marilia at *marilia.wyatt@dowjones.com*.

DOW JONES

WSJ PRO CYBERSECURITY is designed to help executives monitor the ever-changing landscape of cybersecurity through a business lens. Our team of Pro researchers and journalists delivers actionable insight on the wide-ranging challenges of cybercrime risk.

WSJ Pro Cybersecurity membership includes a **daily newsletter, regular panel discussions, interviews, webinars** and **whitepapers** on these business-critical topics:

- Analysis of cyberattacks and their aftermath, including how attackers gained access, how well companies responded and what costs they incurred.
- How companies are preparing for and responding to cyberattacks across all their business functions, including technology, compliance, communications and customer service.
- What companies need to do to adhere to government and state regulations surrounding data, including data governance and disclosure.
- How companies can work with the government to protect themselves against cybercrime.
- What measures small businesses should be taking to defend themselves against cybercrime.



WSJ Pro Cybersecurity also offers **Response Readiness Training (RRT)**, which provides executives knowledge-tools to test their preparedness for cyberattacks in a language they understand: business risk. The non-technical, tabletop exercises will allow decision-makers to identify gaps in response plans, clarify roles and responsibilities and test how their organization would function under pressure.

For more information, visit https://cyber.pro.wsj.com/