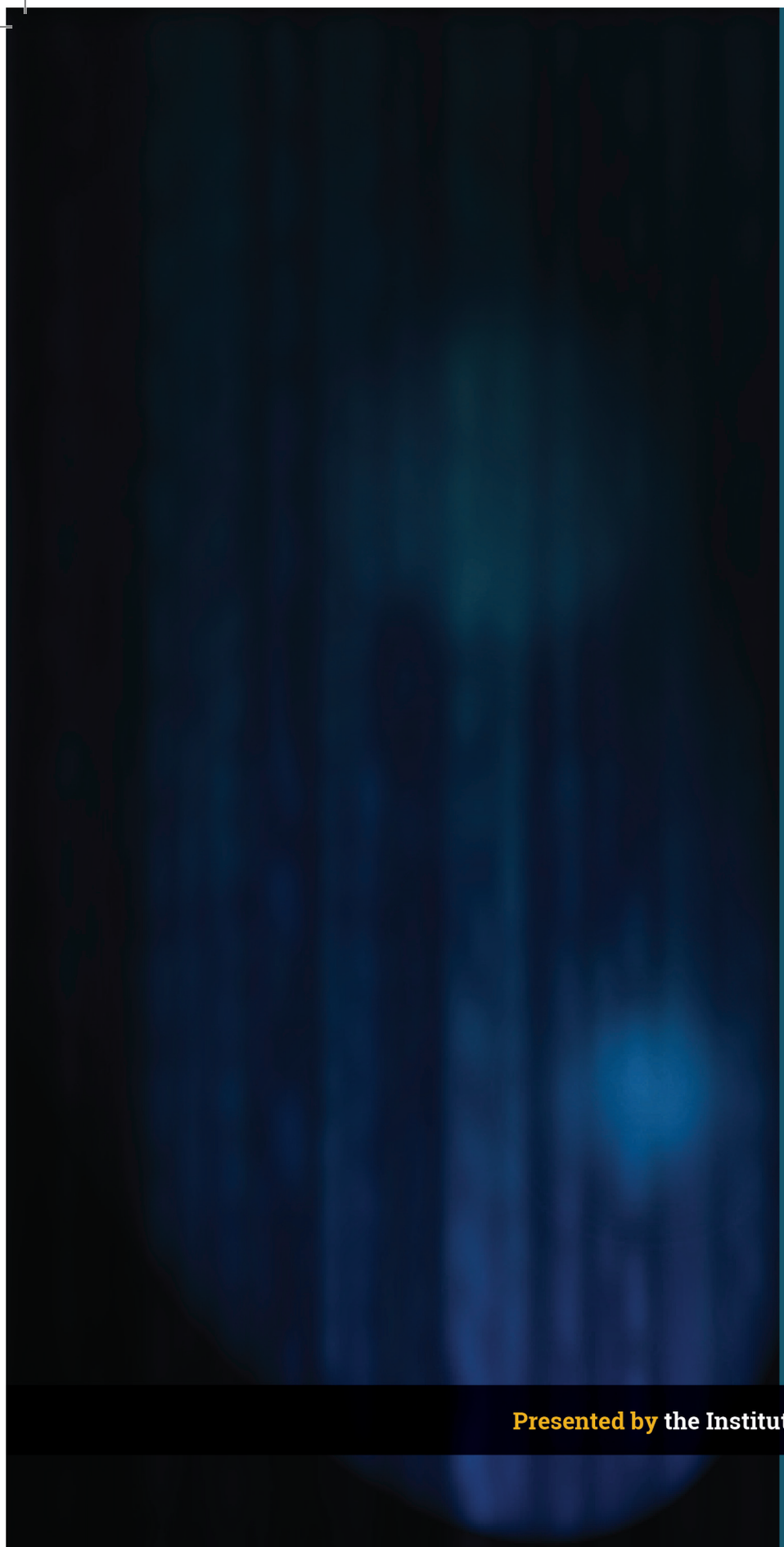


Georgia Institute of Technology

EMERGING CYBER THREATS REPORT 2016

Presented by the Institute for Information Security & Privacy (IISP)

Georgia Tech Cyber Security Summit 2015

Introduction

The intersection of the physical and digital world continued to deepen in 2015. The adoption of network-connected devices and sensors — the Internet of Things — accelerated and was expected to reach nearly 5 billion devices by the end of the year. The collection and analysis of big datasets shed light on a variety of subjects, from profiling consumers' buying habits to forecasting the loss of Arctic ice. Companies, from Google to Apple to traditional car makers, focused greater efforts on creating autonomous vehicles with a near-term goal of a driverless car on the road by 2020.

These trends continue despite obvious dangers. Ever-present devices and online tracking allow us to measure our activities, but give other third-parties unprecedented access to monitor those same habits. Automated systems are increasingly removing humans from operational loops, making everything from driving cars to diagnosing diseases less prone to human error, but at the same time, requiring that each device be trusted — a technology safeguard that does not yet fully exist.

Attackers have shown that these dangers are not just theoretical. Online espionage groups exploited the trust relationship between two background-check suppliers and the U.S. Office of Personnel Management (OPM), leading to the exfiltration of perhaps the most significant cache of U.S.-focused intelligence to date. Two security researchers hacked a GMC Jeep Cherokee while a journalist was driving, resulting in a government-mandated recall of 1.5 million cars.

To understand the dangers posed by our increasingly digital world, we need to study and define both the potential problems and necessary solutions.

The annual Georgia Tech Cyber Security Summit (GTCSS) on Oct. 28, 2015 provided an opportunity for experts from academia, private industry and government agencies to come together and prepare for the challenges we face in securing an ever-more complex society. This is the 13th year that the Georgia Institute of Technology has hosted the event to support efforts to develop bold, new technologies and strategies that ensure the safety and security of government, industry and individuals.

Georgia Tech is one of the nation's top-ranked engineering, computer science and research universities, and it has focused on cybersecurity for more than 20 years. The university houses multiple academic labs dedicated to cybersecurity as well as the Georgia Tech Research Institute (GTRI) — a university affiliated research center (UARC) for the U.S. Department of Defense. Georgia Tech is one of just 13 schools nationwide to receive UARC accreditation from the U.S. government. Its academic labs also hold honors such as National Security Agency Center of Excellence in Information Assurance. Additionally, Georgia Tech has incubated several successful start-ups and has helped make Atlanta a recognized hub for cybersecurity. The university continues to focus on creating the next innovation that will help secure business networks, government systems and personal data.

This year, Georgia Tech amplified its efforts with the launch of an interdisciplinary research institute — the Institute for Information Security & Privacy — to provide a single gateway to our facilities and expertise for those seeking cybersecurity solutions. Georgia Tech's model combines three important elements: 1) academic, discovery-based research that explores new approaches without abandon and encourages uninhibited thinking; 2) applied research involving real-world problems using data shared by external partners, and 3) the ability to move our discoveries into the marketplace for others' benefit. Modern cybersecurity work must take place in these three spheres, and the new Institute for Information Security & Privacy has been built at the intersection of all three.

At Georgia Tech, we understand that bold, new approaches and tactical guidance are needed by so many more than ever before. Leveraging in-house research and expertise, we compiled the following 2016 Emerging Cyber Threats Report. The Report and the Summit provide an open forum for discussion of emerging threats, their potential impact to our digital society, and solutions for a safer and more secure future. We invite you to learn more about our work in cybersecurity and connect with us to discover and solve the grand challenges of today's ever-more connected world.

Wenke Lee
Co-Director of the
Institute for Information Security
Professor, College of Computing

Bo Rotoloni
Co-Director of the
Institute for Information Security
Director, Information and Cyber
Sciences Directorate, GTRI

Consumers continue to lose their privacy as companies seek to collect more data.

Smartphones and wearables make consumers easily trackable, but more advanced technology is collecting digital breadcrumbs beyond what most would want or know.

Highlights:

- To better compete, businesses are focusing on the collection and analysis of Big Data, which can streamline operations and improve marketing, but also poses a significant privacy risk.
- Web sites and advertisers continue to track users behaviors and movements, while consumers have little ability to prevent monitoring.
- The popularity and increased capabilities of connected mobile devices give consumers more features but allow detailed tracking of their habits and movement.
- Advanced computing and pattern-matching capabilities mean data is collected on even the most private citizens.

With a steady stream of breaches hitting the headlines every month, the lack of privacy in the digital world is readily apparent. The custodians of consumer data continue to have problems protecting their customers' information, with companies such as Target and Anthem allowing attackers to steal sensitive customer information.

Unfortunately, people have few options to limit their exposure to data breaches and unintended use of their data. Moreover, most consumers do not know what information companies are collecting on them or how they are using it, says Andrew Howard, director of the Cyber Technology & Information Security Laboratory (CTISL) at the Georgia Tech Research Institute (GTRI).

"There is a general lack of understanding about how much digital dust people are leaving around," he says. "There is a drastic need for two things: Education and technology to focus on the problem."

Businesses are driven to collect more data on consumers to improve operations and lead generation, posing a significant risk to privacy.

The drive to improve business processes and better identify potential customers or markets have businesses collecting as much data they can. Large consumer services, such as Netflix and Amazon.com, regularly collect information to better serve or suggest products to their customers. Others, such as package delivery services and restaurant chains, use data to streamline operations and reduce business costs.

Yet, a whole host of third-party firms, with no relationship to the consumer, also collect data. Visits to the top-100 Web sites, for example, are tracked by more than 1,300 firms, from social networks to advertising networks to data brokers that receive digital dossiers about website visitors and trade them to other businesses.[1]

"Businesses want to collect and collect more information on consumers, but we need to limit them to collecting only the information that is absolutely necessary for the service that they provide," says Wenke Lee, professor of computer science at the Georgia Institute of Technology's College of Computing and co-director of the Institute for Information Security & Privacy (IISP) at Georgia Tech.

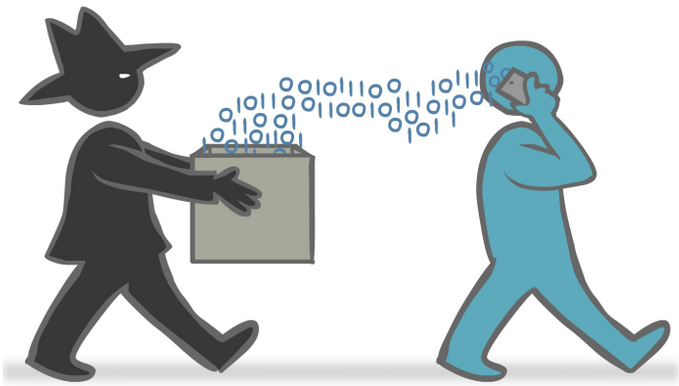
In many cases, a company's access to data may seem legitimate, but the fact that a database exists can often lead to unforeseen and unethical uses of the data. New York City's Department of Transportation, for example, has begun using the E-ZPass trackers, originally intended for collecting automated tolls, as a way to monitor traffic patterns — and by extension, individual drivers — within Manhattan.[2]

In late 2014, the billion-dollar ride-share startup Uber faced criticism for multiple[3] incidents[4] of tracking people without their permission and for making the tracking functionality — known as "God View" — available to workers and prospective employees. In June, the Electronic Privacy Information Center filed a complaint with the Federal Trade Commission charging that the company misled customers about the degree to which they can control their privacy and their ability to opt out of the service's tracking capabilities, among other accusations.[5]

Consumers regularly trade access to their data for convenience.

People are spending a greater amount of time online or on a device. The average U.S. adult spends 2 hours and 34 minutes on a computer or smartphone each day in 2015, up from 2 hours and 1 minute in 2013, according to Nielsen.[6] The digital breadcrumbs that people leave online are allowing companies and governments to form an increasingly detailed picture of their activities.

Mobile devices have accelerated the trend. More companies have access to detailed user data through the installation of apps on smartphones. The average number of installed apps on Android smartphones, for example, has increased by 57 percent over the past three[7] years.[8] Yet, less than 45 percent of those apps are typically used on a monthly basis.[9]



"With smart phones, for the first time in human history, we all carry tracking devices," says Peter Swire, the Huang Professor of Law and Ethics at Georgia Tech's Scheller College of Business.

In April 2015, consumer-monitoring firm Nomi settled[10] a privacy case brought by the Federal Trade Commission, the government watchdog that protects consumers. Nomi's technology allows stores to track consumers' movements through their aisles for marketing and loyalty programs, but the company did not provide any meaningful way for consumers to opt out of their monitoring.

Reversing the trend will be nearly impossible. For one, protecting against monitoring is an almost impossible task for the average consumer, says Noah Swartz, staff technologist for the Electronic Frontier Foundation (EFF). Too often, a person is faced with a choice of agreeing

to the slightly distasteful collection of their data or to being completely unable to sign up for a useful service, an entertaining game or connecting with friends through social media.

“If you find yourself in the situation that you want to use a service or an app, but you don’t agree with the terms of service, you don’t really have to have a choice,” Swartz says. “It is all or nothing.”

In addition, the primary mechanism for notification and consent — privacy policies — have largely failed. Research by Amy Bruckman, professor and associate chair of the School of Interactive Computing at Georgia Tech, and former student Casey Fiesler found that few consumers read online policies and that to do so would take the average Internet user over 200 hours per year.[11]

Advanced computing and pattern-matching capabilities mean even careful citizens are tracked.

Even if a consumer is careful to minimize the information collected by their mobile devices and use pro-privacy technology online, it has become harder to escape notice in the real world. Increased video and signals monitoring of public spaces, paired with the collection of a variety of identifiers — such as license plates, facial images, and smartphone IDs — means that real-world monitoring will increasingly resemble online tracking.

In 2012, the American Civil Liberties Union filed public records requests in 38 states, finding that the technology for reading license plates had already been widely deployed with few regulations on its use to protect citizens’ privacy. Following an outcry from privacy and civil-liberties groups, the U.S. Department of Homeland Security canceled, in May 2015, a planned project to pool license-plate information into a national database.

The debate regarding monitoring policy needs to be public, so that a meaningful debate can focus on the issues, says GTRI’s Howard.

“It’s a policy discussion and a technical discussion,” he says. “I need to know what rights I have, even when I don’t know how many digital breadcrumbs I’m leaving behind.”

What can consumers do to control their data?

While consumers have little control of data once they opt-in to a relationship with a company, there are some ways the average citizen can maintain certain privacy protections.

- Use software that blocks tracking cookies, and delete cookies regularly.

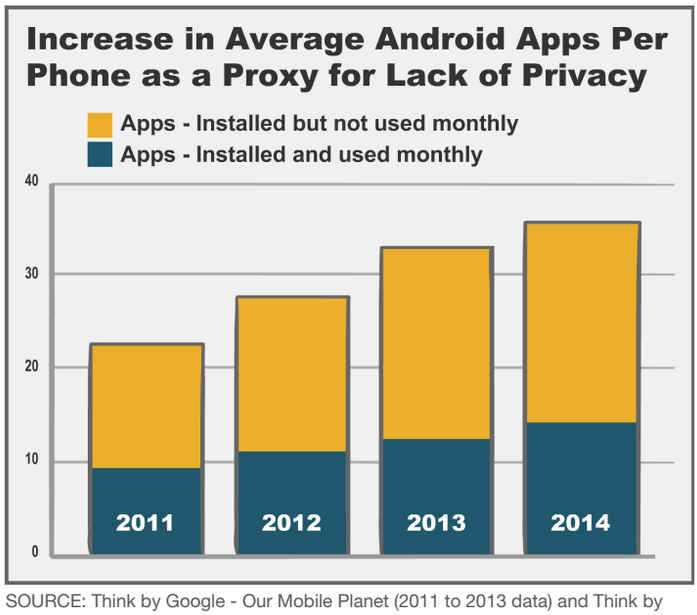
- Use anonymizing networks, such as Tor to defend against network surveillance.

- Be prudent. Don’t download apps unless you need them, delete them once you can, and opt-out of location tracking where possible.

- Don’t use the same password in more than one setting.

- Use back-up systems that you control (such as external hard drives) rather than only cloud-based services.

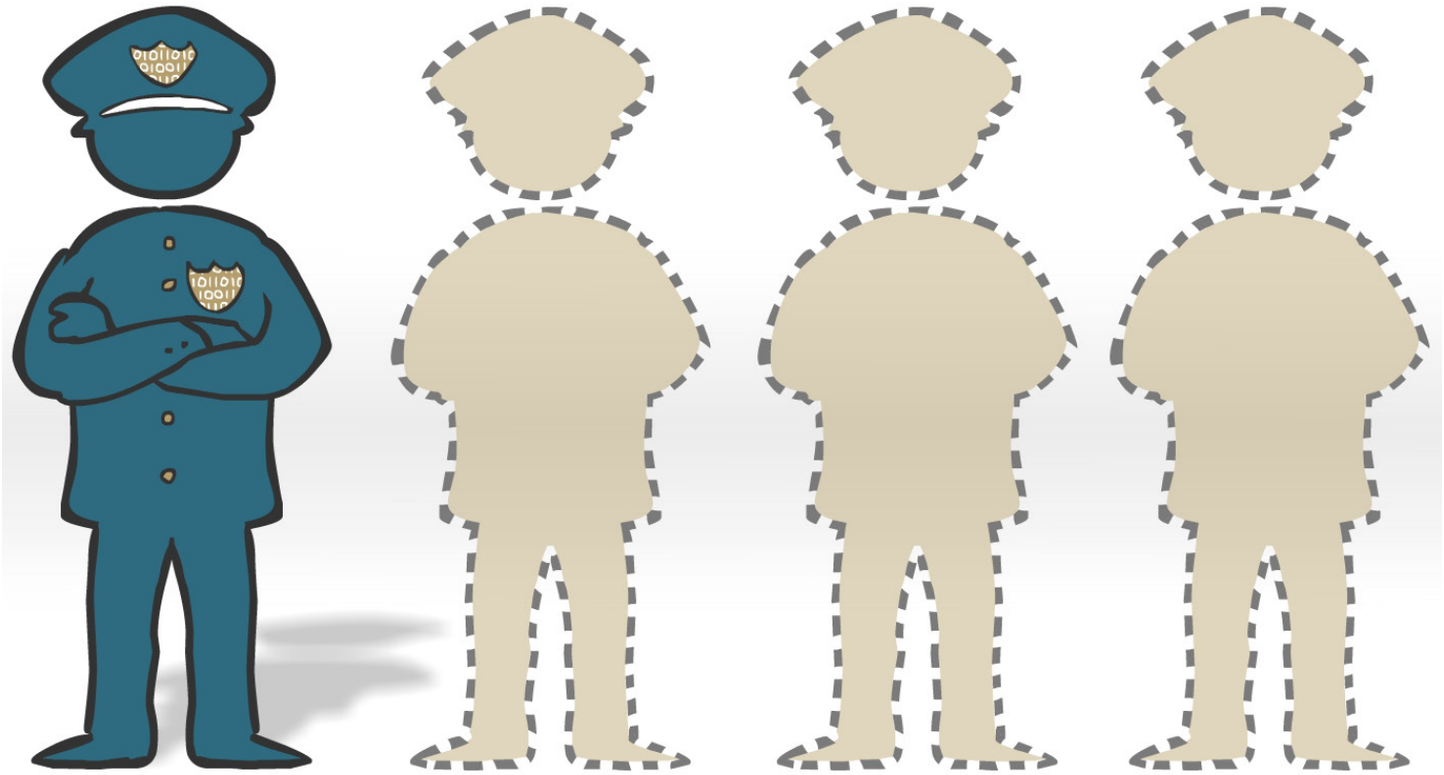
- Support pro-privacy policy groups.



SOURCE: Think by Google - Our Mobile Planet (2011 to 2013 data) and Think by Google Report 2014.

The shortfall in skilled security workers puts companies in peril.

One million information-security specialists are needed to protect data and digital business, but progress promises to be slow.



Highlights:

- Training the domestic workforce fails to produce needed expertise, not only in the United States, but worldwide.
- Boards are increasingly involved in security, but attention to cybersecurity risk varies widely by industry.
- While promising as a way to create voluntary security requirements, cyber insurance continues to face hurdles in assessing risks and the creation of policies that offset business uncertainty.
- The imbalance in the need for security experts and the lack of supply will lead to greater adoption of cloud security services and outsourced security systems as a stop-gap measure.

The infrastructure supporting the digital economy is growing more complex. Companies increasingly run their computing systems on virtual machines, cloud services have become a standard business practices, and personal mobile devices increasingly creep into the workplace.

Yet, despite the influx of technology, there is a significant lack of trained security experts, which will result in a shortfall of as many as 1.5 million workers by 2020, according Frost & Sullivan and the International Information Systems Security Certification Consortium (ISC)2.[12]

“The message that everyone is hearing is, ‘IT everywhere,’ and not just in the online world,” says Mustaque Ahamad, professor in the College of Computing at the Georgia Institute of Technology. “The problem is that ‘IT everywhere’ also requires the need to safeguard IT everywhere, and for that, we need the people.”

The issue affects companies and governments worldwide. The United Kingdom, for example, faces a similar shortfall, with a 2013 report estimating that it will take two decades to address the lack of skilled cybersecurity workers there.[13]

Training of domestic work force falls short, not only for the United States, but worldwide.

Traditional four-year degrees at colleges and universities will not solve the problem. An estimated 18,000 students graduated with a degree in computer science in 2015, the sixth consecutive year of a greater number of graduates.[14] Yet, when compared to the explosion of software ecosystems — there are some 1.5 million apps in the Google Play store alone — those graduates are not enough, especially since most graduates do not have extensive class time in cybersecurity topics.

"Companies are looking for talent and they want that talent to be security aware," says Bo Rotoloni, co-director of the Institute for Information Security & Privacy (IISP) at Georgia Tech.

Five years ago, Intel Corp. began discussing ways to better train college graduates who would be more capable of building secure code. When Intel hires a new computer science or engineering graduate for a security position, it takes about one year to train — or "retool" — them for their work, says Scott Buck, university program manager for Intel.

The company is working with Georgia Tech to develop educational programs and modules that infuse basic cybersecurity concepts into courses taken by all computer science students. Georgia Tech has been at the forefront of addressing the cybersecurity workforce shortage. It offers a master's degree in information security (in both resident and hosted formats) and plans to develop a professional version of this program in the coming year. In addition, a five-course cybersecurity certificate is offered via continuing education, and an entirely online master's in computer science degree (OMS CS) allows students to take cybersecurity courses. Since the pioneering OMS CS program began two years ago, nearly 3,000 students have enrolled and its first graduates are expected in December 2015. More will be needed.

"It is a big ship to try to move," says Buck. "Our programs have just tickled the big ship, just started budging it."

Companies are clearly hungry for information-technology and security talent and are feverishly recruiting students. A wider variety of companies representing more industries — from traditional tech to retail to railroads to paper manufacturers — are coming, for example, to Georgia Tech to recruit. The College of Computing career fair doubled in length this year, to four days, due to the number of interested employers, with record-breaking attendance of 1,683 students in one day.

Security Professional Workforce by Region

Thousands	2014	2015	2016	2017	2018	2019	2014-2019 CAGR
Demand-Meeting Projection							
Americas	1,495	1,673	1,867	2,081	2,308	2,546	11.2%
EMEA	995	1,108	1,230	1,363	1,502	1,646	10.6%
APAC	1,079	1,191	1,320	1,463	1,614	1,771	10.4%
Total	**3,568**	**3,972**	**4,416**	**4,908**	**5,424**	**5,963**	**10.8%**
Supply-Constrained Projection							
Americas	1,418	1,505	1,596	1,692	1,792	1,897	6.0%
EMEA	956	1,013	1,072	1,134	1,200	1,267	5.8%
APAC	1,026	1,076	1,127	1,180	1,235	1,292	4.7%
Total	**3,400**	**3,593**	**3,796**	**4,007**	**4,227**	**4,456**	**5.6%**

SOURCE: Page 33: https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf

Breaches continue to put pressure on executives and workers to emphasize security.

The parade of major breaches over the past three years has gained the attention of corporate boards, not the least because most precede a ritual beheading — the sacking of the CEO. The compromise of retail giant Target, for example, resulted in 110 million records lost and at least $162 million in damages.[15] Lasting less than three weeks, the breach nearly halved year-over-year quarterly profits for the company, resulted in dozens of lawsuits and forced the resignation of Target's then CEO, Gregg Steinhafel, and CIO, Beth Jacobs.[16]

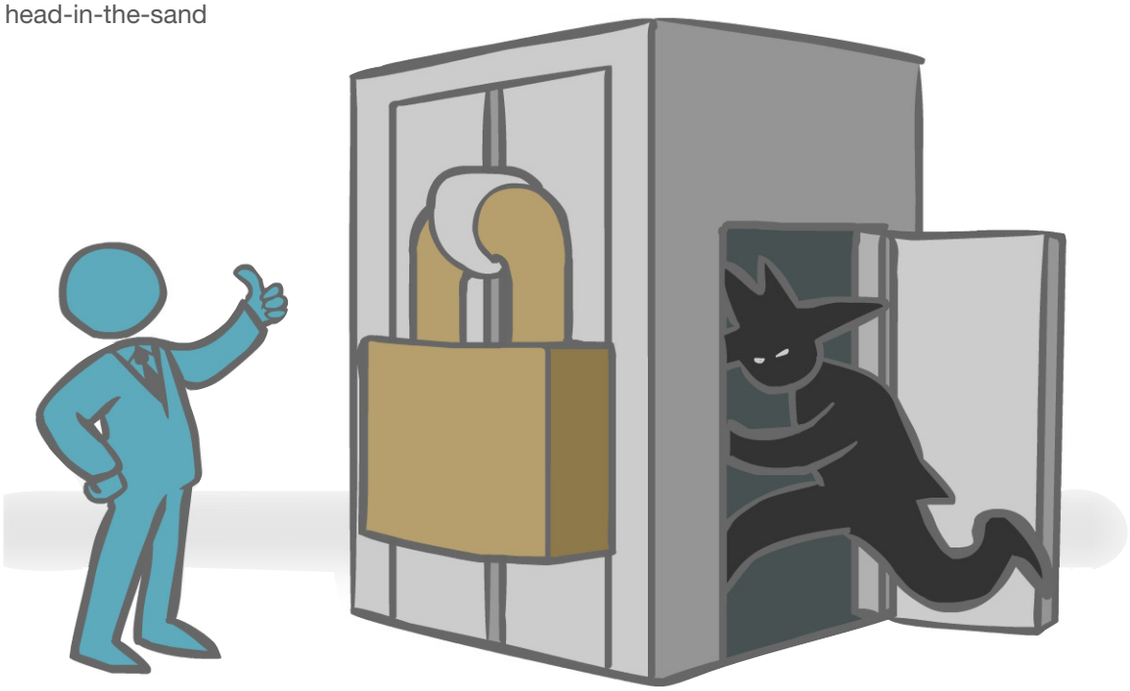
The damage to executives careers has made companies more willing to provide budget to secure the systems and data, says Fred Wright, Principal Research Engineer, GTRI. "The budget for security is certainly easier to argue for these days," he says.

Corporate boards are more focused on security. Over the past four years, the number of corporate filings to the Securities and Exchange Commission (SEC) that have mentioned "information security" have doubled, according to a GTRI survey of nearly 500 filings.[17] In 2015, 63 percent of corporate boards reported actively addressing cybersecurity and risk governance, up from 33 percent in 2012, according to a survey conducted by Jody Westby, adjunct faculty at the College of Computing at Georgia

Tech, and sponsored by Forbes, Palo Alto Networks and Financial Services Roundtable.[18] The survey also found that more than half of chief information security officers report directly to a company's CEO or board.

Yet, businesses have significant room for improvement. The industrial and energy/utilities sectors lag other industries in some aspects of cybersecurity governance, according to Westby's survey. Security needs to be adopted from the executive offices all the way down to workers' cubicles.

"As we get people who are more aware of security as a problem, then decisions about strategy and approach are going to improve," Wright says. "And rather than a head-in-the-sand approach, the whole organization will drive toward a more secure posture."



While many companies are focused on the security threat posed by disgruntled workers, almost all companies need to be worried about the threat posed by well-intentioned workers who do not understand security. Former National Security Agency contractor Edward Snowden underscored the danger of the insider threat, yet many breaches start with an employee ill-advisedly opening a phishing e-mail, says Noah Tobin, research associate with GTRI's Cyber Technology and Information Security Lab (CTISL).

"When most people think of an insider threat, they think of Snowden, but there is also the unintentional insider threat," Tobin says. "They are using their work e-mail to sign up for websites, for example, which lets it out that the person works at an organization, and hackers can target that."

Companies need to focus on educating their employees about security issues — teaching them about the dangers of phishing, unencrypted data and lax reactions. Training employees can turn a worker into a security asset, capable of helping detect threats, rather than a liability.

Additional policies may be needed as well. Companies should, if appropriate, clamp down on personal use of employer-issued devices to minimize threats or monitor the use of consumer devices inside the workplace.

The market imbalance will lead to greater adoption of automation, cloud security services and more intelligent security systems.

With education and training requiring years, and possibly decades, to address the current shortfall of skilled security specialists, technology and businesses must fill the gaps in the short term. While educating the future generation of security professionals is necessary, it is a long-term solution. In the short term, using cloud and security services to deliver security expertise to a broad base of companies may be the only way forward.

More intelligent security systems that improve the

recognition of important security alerts can help businesses better secure their networks and data. A decade ago, companies were just starting to mine their systems' log files for security information and required a team to maintain the capability. Today, such tools consume much more data from a greater variety of IT devices and do much of the initial work to eliminate false alerts.

"Automation is a big one," Wright says. "We can reduce the workload by better analysis using more data to reduce false positives. Then we can help find more sophisticated threats."

Automation is not just about improving software. Businesses that bring the benefits of automation into security services can help create a foundation of security for client companies. Security-as-a-service can allow a single expert to maintain and administer multiple clients, reducing the demand for security experts. Through automation, advanced analytics and a highly trained workforce, security-as-a-service provider Dell SecureWorks filters through more than 150 billion events a day for its 4,200 clients, and whittles them down to about 10 billion security events. Those events are then correlated, analyzed, and reduced to less than 5,000 potential attacks that require a response, according to the firm.

Through that sort of specialized automation, tools and analytics, a single security worker at a security-as-a-service provider can be far more productive than a lone worker at even a security-savvy firm, says Jon Ramsey, chief technology officer for Dell SecureWorks.

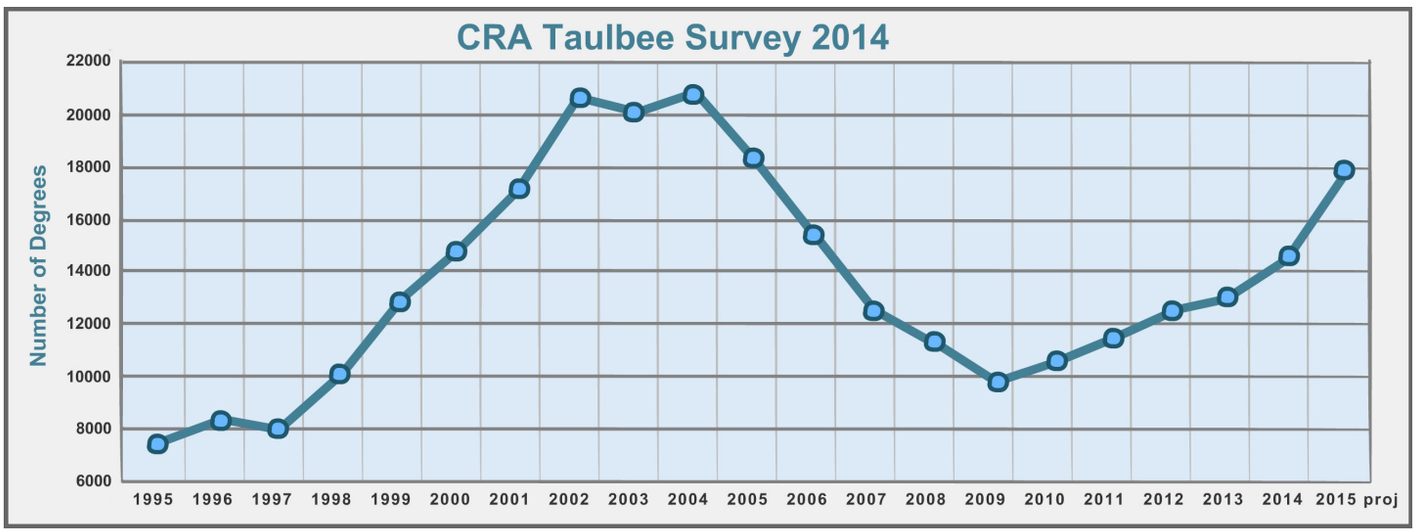
"Managed security service providers are necessary, because we are not going to solve these problems in the short term, and maybe not in the medium term either," he says.

Will insurance work to improve security?

As more breaches expose more business and consumer information, cyber insurance has taken off. By 2025, the market will grow to more than $20 billion.[19]

Cyber insurance has its problems, however. Policies continue to have a large number of exceptions, leaving many firms to question whether the insurance company will pay in the event of an incident. In May, for example, CNA Financial Corp., sought a judge's ruling that the insurance company did not have to pay $4.1 million to non-profit healthcare organization Cottage Health Systems (CHS).[20] The insurance company has a point, however: The lawsuit claims that CHS, or a third-party storage provider, failed "to follow minimum required practices," leaving data accessible to the Internet and unencrypted.

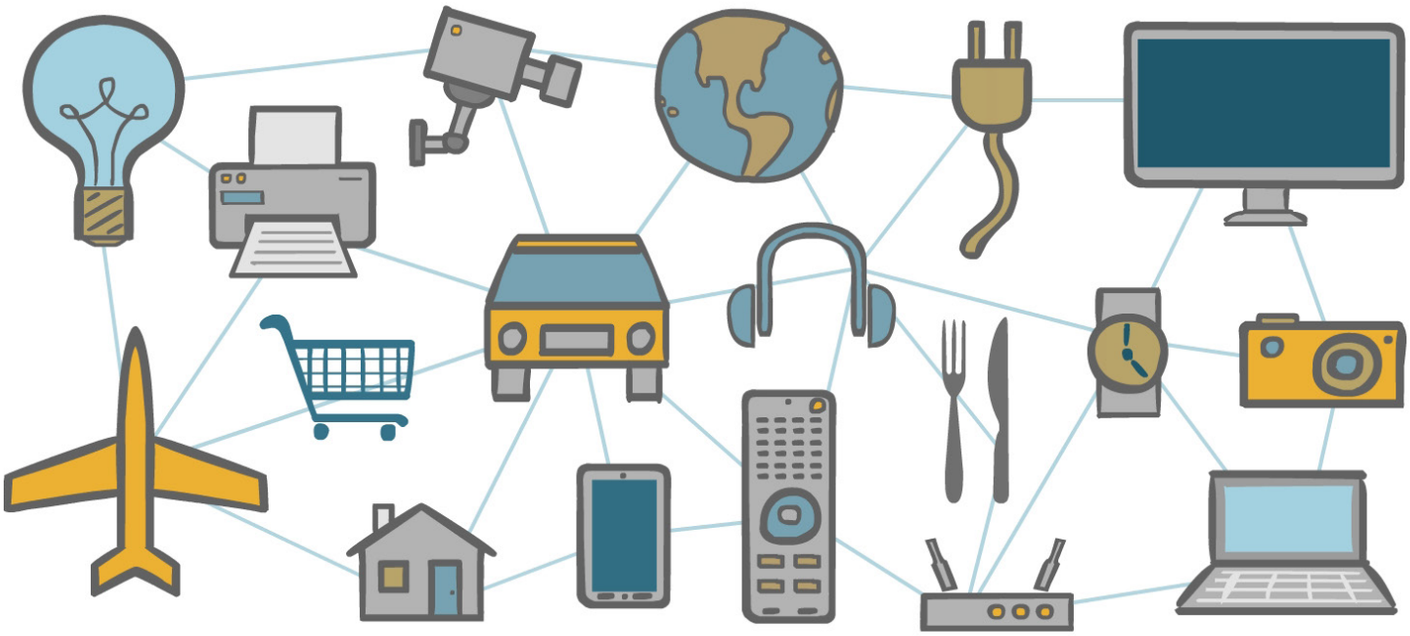
Buying an insurance policy — although alluring — may not excuse a business from obligations to reasonably protect its data.



SOURCE: Page 24: http://cra.org/wp-content/uploads/2015/06/2014-Taulbee-Survey.pdf

Security and trust problems continue to plague cyber-physical systems.

The growth of the Internet of Things and complexity of industrial control systems will lead to more vulnerabilities in hardware systems.



Highlights:

- With the Internet of Things expected to grow to between 25- and 50-billion devices by 2020, businesses and consumers will face a larger attack surface.
- Security researchers and attackers increasingly focus on finding vulnerabilities in industrial control software, putting such systems in greater peril.
- Securing the supply chain continues to be difficult, relying on a complex multi-disciplinary effort to make work.
- As devices, systems and appliances increasingly communicate, verifying trust becomes a fundamental, and yet-to-be-solved problem.

Connected devices are becoming a greater part of our lives. From exercise-tracking devices to smart watches to sensors for monitoring industrial processes, businesses and consumers are using connected devices — the so-called "Internet of Things" or IoT — to collect information from the world around them and manage their lives and businesses. The Internet of Things will become such a part of our lives that people "won't even sense it, it will be all around you," Google CEO Eric Schmidt told the World Economic Forum in Davos, Switzerland, in January.[21]

Yet, attackers are increasingly looking for vulnerabilities in both the IoT and industrial control systems to gain access to targeted data and systems. The Stuxnet attack on Iran's nuclear capability in 2010, for example, highlighted the danger to industry control systems' (ICS) software and devices. A variety of research into home automation and wearable sensors have spotlighted similar problems for consumer devices, with studies from Hewlett-Packard, Symantec and IOActive finding serious security issues in

consumer devices, automotive systems, and home-automation systems.[22]

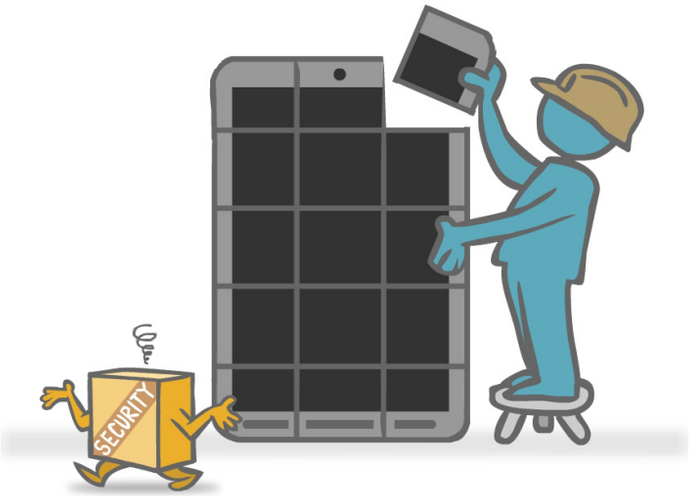
With devices and sensors finding their way into every industry and aspect of consumers' lives, security needs to become a higher priority, says A.P. Meliopoulos, the Georgia Power Distinguished Professor of Electrical and Computer Engineering at the Georgia Institute of Technology.

"We are seeing the same thing with other physical systems," he says. "Transportation, health systems, robotics — Everything is converted into the cyber-domain and that increases the number of entry points for attack."

Growth of Internet of Things and proliferation of mobile devices leads to a larger attack surface.

The number of connected devices and sensors is exploding. In 2007, excluding smartphones, approximately 10 million sensors and devices communicated over a network.[23] Currently, an estimated 5 billion such devices are now connected — a number that will continue to dramatically climb over the next decade, although estimates vary from 25 billion[24] or 50 billion[25] by 2020 to 1 trillion devices by 2025.[26]

The explosion in the number of devices has not resulted in manufacturers paying much attention to security. A small-sample study by Hewlett-Packard found that 7 out of 10 tested devices — including a smart TV, home thermostat, and connected door lock — had serious vulnerabilities that could be attacked.[27] A 2014 study by Symantec found that a $75 scanner could capture private or sensitive information from exercise trackers and other wearable devices.[28]



"No one wants to build security into their devices, because no one is going to pay more for a secure device," says Bo Rotoloni, co-director of the Institute for Information Security & Privacy (IISP) at Georgia Tech. "So these device manufacturers do not naturally have security in their mind set, which leads to an engineering staff who are not properly trained."

Yet, coming up with a single approach to improve the security of the Internet of Things is difficult, and currently the best way to secure devices is for the manufacturer or concerned customers to audit devices to ensure trust. As of yet, that is no easy task.

"It has to change, but it is not changing yet," says Diane Stapley, director of alliances for processor maker Advanced Micro Devices, Inc., (AMD). "There is so much focus on getting a product out the door, that security is not a focus among the developers, so security has to be built in at design, or the update cycle needs to be created to make the devices field upgradable."

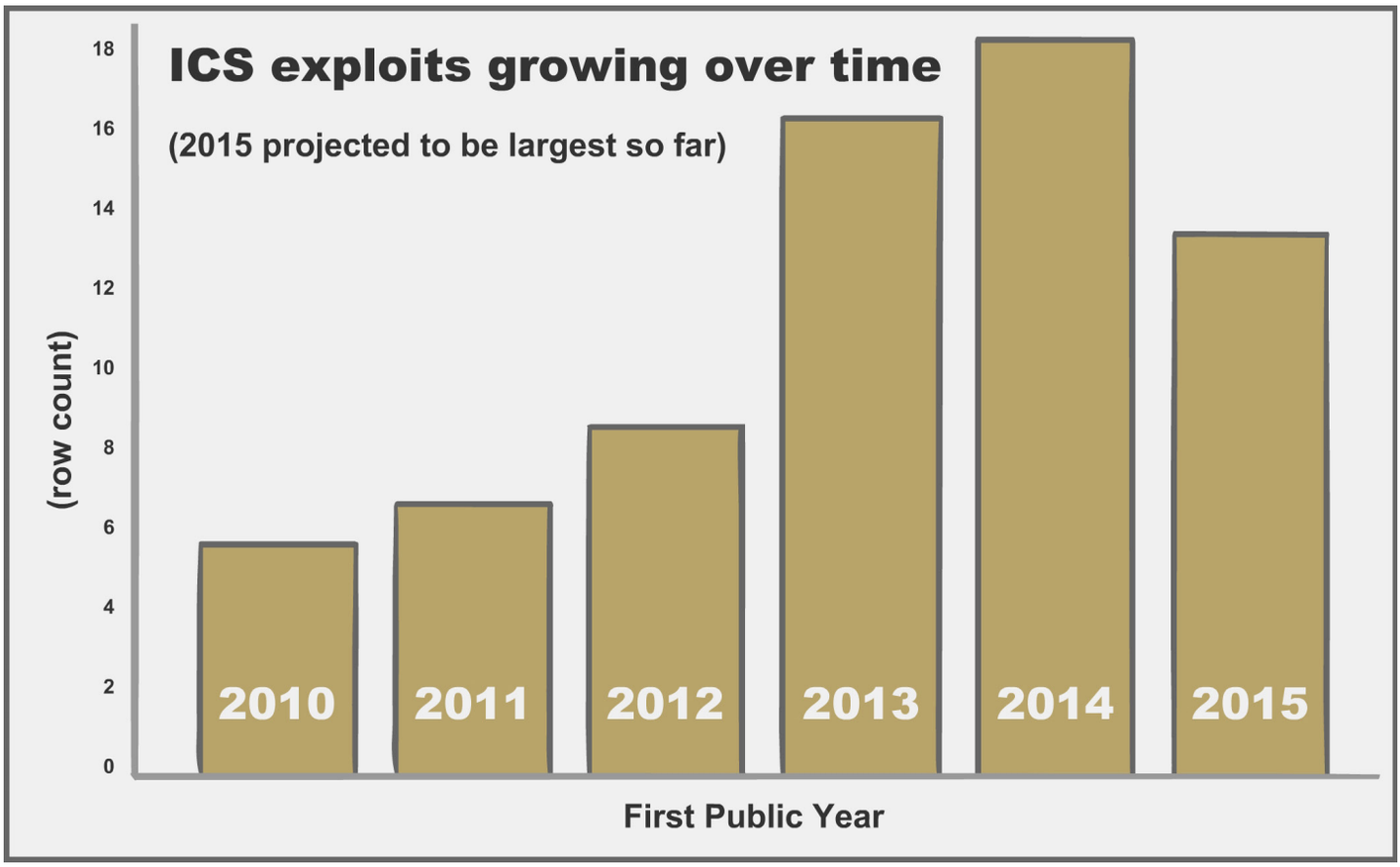
Industrial control systems are a growing focus of vulnerability research and attacks.

Industrial control systems (ICS) face similar problems. Prior to the discovery of the Stuxnet attack in 2010, security researchers and vendors reported less than 10 vulnerabilities in industrial control systems annually. In 2011, however, that changed. Nearly 50 vulnerabilities were reported that year, followed by an average of 100 vulnerabilities for the next three years.[29] Worse, the exploitation of ICS vulnerabilities has climbed from six in 2010 to 19 in 2014, according to Recorded Future.[30]

With such systems being used in a wider variety of settings, mitigating the vulnerabilities will become increasingly important.

"A few decades ago, industrial control systems were fairly limited, but now their functionality is expanding and they are being applied to new applications, such as home automation," Meliopoulos says. "We are moving in a direction now, where the only things not in the cyber domain are the analog parts of an actual physical system."

In 2015, Georgia Tech's School of Computer Science began a project for the Office of Naval Research to create a penetration test "in a box" for industrial control systems.



SOURCE: Recorded Future. "Up and to the Right: ICS/SCADA Vulnerabilities by the Numbers." Recorded Future Threat Intelligence Report. 9 Sep 2015. PDF. Study-2015.pdf. http://go.recordedfuture.com/hubfs/reports/ics-scada.pdf

"Assessing the security of industrial control systems today often takes the form of a 'penetration test' that requires someone familiar with security practices, reverse engineering, real-world exploitation and the intricacies of a particular industrial domain," says primary investigator Dr. Wenke Lee. "All of that is rare in a single team or person, so we've proposed an end-to-end system that can automatically detect, and adapt inside new systems and networks." Lee will work with Associate Professor Taesoo Kim on this project, expected to be complete in 2018.

As devices, systems and appliances increasingly communicate, verifying trust becomes a fundamental problem.

As devices connected through the Internet of Things proliferate, the world will be facing increasingly serious trust issues. Smartphones, which have become the mobile hub of people's lives, must have ways to determine how trustworthy, for example, a fitness band or a wireless speaker might be. Home routers or automation hubs will have to determine whether they trust a new security camera or an intelligent thermostat.

While humans learn how to determine if another person or thing is trustworthy — based on information gained through perception, memory and context — whether those concepts can be transferred to the digital realm is still an active area of research. Machine-to-machine (M2M) trust is increasingly important, rather than trusting the channel through which machines communicate with one another.

The issues will become even more critical as digital technologies become an increasing part of our lives, such as some technologists' dreams of self-driving cars. Such vehicles will have to communicate with each other and be able to distinguish spoofed communications or illogical commands. All of this has to be done automatically without human intervention, says Georgia Tech's Rotoloni.

"Communication channels are going to be intermittent, so you have to be able to operate with resilience," he says. "If you have a car next to you, you might trust that car a little less if you know it has not been updated with the latest software patches."

How do we determine trust today? Challenges of the supply chain

Today, trusting hardware, devices and data boils down to establishing a chain of trust, from the provider of the device or data to the method of delivery to the administrator of the asset. Each step requires verification, vigilance and the ability to detect changes to processes or devices.

In the physical world, those activities have to be audited to ensure only trusted parties are handling the device or data. In the digital world, trust is established through digital certificates, encryption and other information-security technologies. Yet, weaknesses in this infrastructure are apparent. About 4.4% of all malware is signed using developer certificates as a way to circumvent (see next section) and domain registrars have often been fooled into issuing fake online certificates.

Even established Internet service providers can be fooled by weaknesses in routing protocols that make it possible for malicious actors to hijack traffic. The National Science Foundation has tasked Georgia Tech with solving the trust problem between ISPs in a multi-year project that will redefine Internet routing protocols to verify the true owner of a network and to validate the international chain of legitimate network paths. In its first year, the work is led by Russ Clark, professor of computer science, and researchers at Georgia Tech's Office of Information Technology.

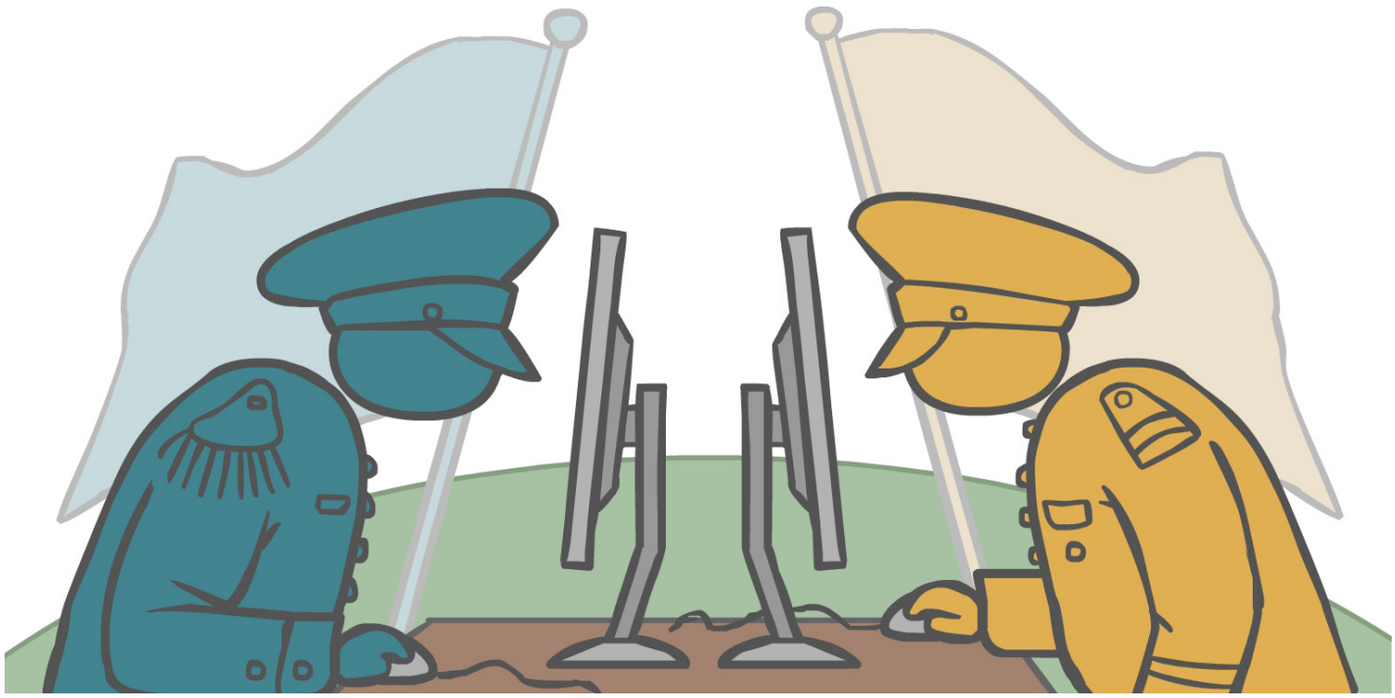
PROJECT: Establishing trust in critical embedded processes

To protect critical cyber-physical system processes, Georgia Tech is developing a technology called Trustworthy Autonomic Interface Guardian Architecture, or TAIGA, to establish trust at the embedded-control level. The architecture creates a small root of trust that sits between physical processes and an embedded controller and maintains known good states. The code for the device is small, so it can be formally verified, and its implemented in hardware, which has additional performance and security benefits.

"Once we have a known good state, that is we have some sense of how the physical systems should behave in a stable or secure manner, we can enforce that via our root of trust," says Lee Lerner, research faculty at GTRI. "Our threat model ensures TAIGA can enforce certain physical characteristics regardless of what all other cyber systems are doing."

Information theft and espionage shows no signs of abating

With few penalties if they are caught, nations continue to conduct online operations to steal information and gain advantage over their rivals, causing real economic impact.



Highlights:

- Cyber operations — not just financially-motivated criminal activity — have become commonplace, with dozens of nations conducting some intelligence operations in cyberspace.
- Threats continue to advance, adding anti-analysis functionality and incorporating modularized components — such as stolen digital signatures — to defeat defenses.
- Not only are malicious cyber operations relatively inexpensive and actors unlikely to get caught, but few disincentives for cyber espionage exist, making it likely that activity will continue to increase.
- Unrestricted expansion of espionage in cyberspace could, along with cybercrime, create a significant drag on the world economy.

In late 2013, a group of attackers began to target the networks of the U.S. Office of Personnel Management (OPM), first stealing manuals for its information-technology networks and then compromising two contractors who conduct background checks of potential federal workers.[31] While OPM officials believed they had stymied several attacks, the operations continue, eventually resulting in a December 2015 breach that resulted in the loss of the digital files documenting background checks on all current and potential federal employees and contractors. The Obama administration has named China[32] as the perpetrator, making the breach arguably the worst data loss attributed to a nation-state to date.

The Internet has become an intelligence battleground for every nation seeking an advantage on their rivals. The OPM breach is only the latest attack. In 2010, the United States and Israel are believed to have cooperatively attacked Iran's nuclear processing capability using the Stuxnet program[33], which kicked off the Iranian

government's quest for better cyber capabilities. Russian actors have been active since at least 2008, developing and using a flexible espionage platform, according to recent research released by Finnish antivirus firm F-Secure.[34] Other nations have developed their own capabilities, or purchased them from offensive-tools providers.

Without an effective deterrence, the operations will continue to escalate, says Lee Lerner, research faculty at Georgia Tech Research Institute (GTRI).

"The cyber-physical systems landscape, in general, is the future of modern warfare," he says. "I think there will increasingly be a game played between nations — how much can you subtly disrupt physical infrastructure via cyberattack without it amounting to an act of war?"

Michael Farrell, chief scientist for GTRI's Cyber Technology & Information Security Lab, believes the digitization of physical data – such as fingerprints, iris scans, palm geometry, and other biometrics – could lead to an increase in theft of these unique signatures. According to Farrell, there is an opportunity to leverage this data and it is too early to tell whether the bigger impact will be for good (e.g. broad adoption of strong authentication) or evil (e.g. fraud).

"Either way, this digitization and storage of these personal signals is an area ripe for innovation," says Farrell. "Personally identifiable information (PII) is now more than just your date of birth (DOB) or social security number; (SSN); your fingerprints and iris scans are now sitting in relatively unprotected databases on highly connected systems."

If no way is found to deter cyber-espionage and cybercrime, the drag on future potential benefits to the economy could be significant — as much as $90 trillion in 2030, according to a report[35] published by the Atlantic Council and the Zurich Insurance Group.

International cyber operations — not just financially-motivated criminal activity — have become commonplace.

While cybercrime continues to be the most prolific malicious activity on the Internet, nations and groups operating on behalf of national interests continue to expand. A great deal of cyber-espionage activity is attributed to Chinese actors. Yet, groups affiliated with France, Israel, Iran, Russia, Syria, the United Kingdom, and the United States all have been documented. Documents leaked in a breach of offensive-tools provider Hacking Team indicate that the company sold surveillance tools and services to intelligence services in Azerbaijan, Kazakhstan, Uzbekistan, Russia, Bahrain, Saudi Arabia and the UAE[36], among other nations.

Over the past five years, cyber operations have evolved from gathering competitive intelligence to focusing on more general information about people. In the past year, attacks on both the OPM and healthcare provider Anthem, Inc., have been linked to the Chinese. The information is already being mined by both China and Russia to uncover intelligence operatives.

"You have a huge swath of industry that will be hacked for national security purposes," says Dmitri Alperovitch, CTO and co-founder of cybersecurity technology firm CrowdStrike. "They all fall into the security realm, and those types of intrusions will escalate."

In addition to digging deeper into the details of potential target, nations are increasingly focused on examining the weaknesses in critical infrastructure. In a study of the interest in Internet-exposed critical information systems, one security firm found that two-thirds of attacks on the fake systems came from Russia and China, and nearly half of all critical attacks came from China.[37]

"Nations are not just going after the data anymore, they are trying to affect functionality," Lerner says. "This threat is especially relevant to embedded systems, which typically contain little protections yet often serve critical functions."

Farrell agrees. "Safety will be a key driver of progress in the cyber security of operational technology, such as industrial control systems."

Threats continue to advance, adding anti-analysis functionality and incorporating modular components — such as stolen digital signatures — to defeat defenses.

Attackers continue to seek ways to make their code harder to detect and analyze. Signing code using developer certificates is the accepted way for programmers to signal that their applications are official. However, attackers frequently steal certificates and then use them to sign their own spyware and malicious code. A study by Intel Corp.'s security arm McAfee found that 4.4 percent of attackers sign their code.[38]

The reality for users and security professionals is that preventing attacks is increasingly difficult. In response, organizations are finding ways to blunt the impact of breaches with techniques such as deceptive networks or comprehensive encryption.

"You can't stop the breaches, it is a fool's errands to stop the breaches," says David Bader, researcher and chair of the School of Computational Science & Engineering at the Georgia Institute of Technology. "That is where we are worried about malware and hackers and passwords."

Attackers are advancing in other ways as well. Nation-states are experimenting with disinformation campaigns. On the 2014 anniversary of Sept. 11, text messages were sent to local Louisiana residents stating that an explosion at a chemical plant had released toxic fumes. Hundreds of fake Twitter accounts — and a forged video on YouTube — soon followed with similar messages.[39]

But nothing had actually happened. The campaign was an elaborate hoax, at best, or a test of the capabilities of the Internet to be used for disinformation, at worst. Other hoaxes, linked to Russian groups, have followed. Other nations are also employing disinformation, hiring armies of "trolls" to spread propaganda to the Internet.[40]

Deterring cyber espionage remains a key concern.

Unfortunately, there are no easy solutions for responding to nation-state espionage or cyberattack. As long as governments are able to plausibly deny involvement, disincentives are limited.

"Our current level of deterrence is not deterring anyone," says Michael Farrell, chief scientist of the Cyber Technology and Information Security Lab at GTRI. Citing recent Congressional testimony by Admiral Michael S. Rogers,[41] director of NSA and head of the U.S. Cyber Command, Farrell points to an ongoing debate about the need for a stronger offense but an uncertainty among U.S. policymakers about when and how to use it. Geopolitical realities and the interconnected nature of the global economy dissuade Western nations from using the "soft" levers of power, such as sanctions and embargoes.

"We indicted five guys who will never see the inside of an American court and who have likely kept on hacking," Farrell says. But he adds that this public indictment may have provided the White House with leverage for reaching an agreement with China on curbing economic espionage at the end of September 2015.

The lack of a kinetic response to the Sony Pictures hack in 2014 also has been interpreted by some as a sign of how poorly America will to respond to cyberattacks.

Policy makers continue to debate what constitutes appropriate deterrence to attacks in cyberspace. Farrell believes that cyber deterrence will likely not operate like nuclear deterrence.

"Nuclear deterrence was primarily a military strategy designed to prevent one completely unacceptable outcome — nuclear war with the Soviet Union," he says. The great power conflict comparison is misunderstood, Farrell believes. "There are differences between Russia and China that span economics and technology. Unlike Russia, there is significant US-Sino trade integration, as well as American dependence on China for many parts of the supply chain."

Cyber deterrence may require the concurrent use of political, economic, diplomatic, and military tools with the realistic goal not to stop attacks entirely, but instead to reduce the volatility and intensity of cyber operations in future conflicts.

"Without a doubt, the law of armed conflict must evolve and be context dependent," says Farrell.

He recounts two key elements of 20th century history. The idea of attacking commercial shipping was abhorrent in the early 1900s, and this idea prompted America's entry into WWI. Then after the attack on Pearl Harbor in December 1941, American policy changed in less than a day to not

only permit but directly task the US submarine fleet to sink non-military ships. The evolution of reactions to attacks in cyberspace may evolve in a similar fashion, he says.

In the absence of a strong deterrence strategy, information sharing becomes even more important as a way to bolster defenses. Better intelligence sharing could help companies collaborate on defending against attacks, but only if a workable solution can be found.

The quality of commercial threat intelligence has risen dramatically in the past two years, according to Farrell, with companies such as iSight Partners, Cyveillance and Dell SecureWorks offering a range of tailored threat intelligence products, and other companies — such as ThreatConnect, AlienVault's Open Threat Exchange and HP's Threat Central — offering services to support collaboration between industry peers.

"We need to create an ecosystem where everyone is playing well together," said Jason Belford, associate director of Georgia Tech Cyber Security.

To be most effective, threat intelligence should be consumed in three tiers. Tactical threat intelligence has to be easily shared, machine-to-machine, to avoid delays. Operational threat intelligence should be leveraged by corporate IT security analysts in a security operations center (SOC). Strategic intelligence must be in the hands of senior decision-makers who are driving business operations and making resource decisions.

When it comes to community-based info sharing programs, however, there is still work to be done, says Farrell.

"Unfortunately, many companies just aren't ready for a robust information sharing program," says Farrell. "They know about it, and many are trying to ingest a feed or two, but few have the resources of Facebook or Google to devote to a program in which they also share out (publish) actionable information in a useable format."

Attribution no longer a problem?

While the attribution of attacks is often described as an inexact science, with the possibility of attackers using misdirection to throw analysts off the trail, most security experts believe there have been few missteps. While technical analysis can suggest a perpetrator, most commercial offerings today derive attribution statements from a blend of manual analysis of forensic and circumstantial evidence. Perpetrators often leave behind traces of network and host-based activity that can be correlated with other open source intelligence sources to paint a picture of what transpired.

"Attribution is an extremely difficult problem when the goal is 100 percent certainty and the methods used must be scientifically robust," says GTRI's Farrell. "We are collaborating across campus to bring machine learning techniques to bear against large malware libraries, commercial and public traffic logs, open source indicators of compromise, and other data repositories. Our goal is to leverage results from multiple domains of evidence to provide context necessary to reduce uncertainty in

Cybersecurity mentions in corporate SEC filings, 2010-2014

	Cyber	Hack	Information Security	Cyber or Information Security
2014 499 filings	329	193	126	351
2013 497 filings	265	155	109	294
2012 496 filings	185	139	98	226
2011 496 filings	62	95	70	115
2010 496 filings	39	76	64	90

SOURCE: Unpublished Research. King, James. GTRI. October 1, 2015.

References

[1]"Getting to know you." The Economist. The Economist Newspaper Ltd., 13 Sep 2014. Web. 11 Sep 2015.

[2]Hirose, Mariko. "Newly Obtained Records Reveal Extensive Monitoring of E-ZPass Tags Throughout New York." ACLU.org. American Civil Liberties Union, 24 Apr 2015. Web. 28 July 2015.

[3]Sims, Peter. "Can We Trust Uber?" Silicon Guild. Medium, 26 Sep 2014. Web. 9 Sep 2015.

[4]Bhuiyan, Johana and Warzel, Charlie. "'God View': Uber Investigates Its Top New York Executive For Privacy Violations." BuzzFeed. BuzzFeed Inc., 18 Nov 2014. Web. 9 Sept 2015.

[5]"In re: Uber Privacy Policy." EPIC.org. Electronic Privacy Information Center, n.d. Web. 9 Sep 2015.

[6]The Total Audience Report - Q1 2015. Nielsen. PDF. 10.

[7]"Our Mobile Planet." Google, n.d. Web. 2 Sep 2015. Data from 2011 to 2013.

[8]Google. Mobile App Marketing Insights: How Consumers Really Find and Use Your Apps. 2014 data. May 2015. PDF.

[9]Google. Mobile App Marketing Insights. 2014 data is extrapolated.

[10]Federal Trade Commission. "Retail Tracking Firm Settles FTC Charges it Misled Consumers About Opt Out Choices." FTC Press Release. FTC, 23 April 2015. Web. 28 Sep 2015.

[11]Singer, Natasha. "Didn't Read Those Terms of Service? Here's What You Agreed to Give Up." The New York Times. The New York Times Co., 28 Apr 2014. Web. 28 Sep 2015.

[12]Frost & Sullivan and (ISC)2. "The 2015 (ISC)2 Global Information Security Workforce Study." Frost & Sullivan, 16 Apr 2015. PDF.

[13]"National Audit Office warns UK needs more skilled cyber-crime fighters." BBC.co.uk. British Broadcasting Corp., 12 Feb 2013. Web. 8 Sep 2015.

[14]Zweben, Stuart and Bizot, Betsy. 2014 Taulbee Survey. Computer Research News (Vol. 27, No. 5). Computing Research Association, May 2015. PDF.

[15]Lunden, Ingrid. "Target Says Credit Card Data Breach Cost It $162M In 2013-14." TechCrunch. AOL Inc., 25 Feb 2015. Web. 17 Sep 2015.

[16]Lemos, Robert. "5 Steps To Supply Chain Security." DarkReading. UBM, 6 Aug 2014. Web. 12 Sep 2015.

[17]King, James. Unpublished research on SEC filings. Georgia Tech Research Institute, 1 Oct 2015.

[18]Westby, Jody. Governance of Cybersecurity: 2015 Report. Palo Alto Networks, Financial Services Roundtable, Forbes, Global Cyber Risk LLC, 2 Oct 2015. PDF.

[19]Allianz Global Corporate & Specialty. A Guide to Cyber Risk. Allianz, 9 Sep 2015. PDF. pg. 5.

[20]Greenwald, Judy, "Insurer cites cyber policy exclusion to dispute data breach settlement." Business Insurance. Crain Communications, 15 May 2015. Web. 15 Sep 2015.

[21]Agence France Presse. "Internet Will 'Disappear', Google Boss Tells Davos." NDTV. NDTV Convergence Ltd., 24 Jan 2015. Web. 20 Sep 2015.

[22]Lemos, Robert. "Internet of Things security check: How 3 smart devices can be dumb about the risks." PCWorld. IDG Consumer, 18 Feb 2015. Web. 20 Sep 2015.

[23]Stanford University. "T-Sensor Summit for Trillion Sensor Roadmap." T-Sensor Summit. Stanford University, 23 Oct 2013. PDF.

[24]Gartner. "Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015." Gartner press release. Gartner Inc., 11 Nov 2014. Web. 15 Sep 2015.

[25]Cisco. "Seize New IoT Opportunities with the Cisco IoT System." Cisco Web site. Cisco, n.d. Web. 15 Sep 2015.

References

[26]See collection of estimates in T-Sensor Summit Roadmap, p. 1.

[27]HP Fortify. “Internet of Things Research Study: 2014 Report.” Hewlett Packard, 29 Jul 2014. PDF.

[28]Symantec Security Response. “How safe is your quantified self? Tracking, monitoring, and wearable tech.” Symantec, 30 Jul 2014. Web. 20 Sep 2015.

[29]Recorded Future. “Up and to the Right: ICS/SCADA Vulnerabilities by the Numbers.” Recorded Future Threat Intelligence Report. 9 Sep 2015. PDF.

[30]Cyber Threat Intelligence Group. “Web Data Reveals ICS Vulnerabilities Increasing Over Time.” Recorded Future Blog. Recorded Future, 9 Sep 2015. Web. 18 Sep 2015.

[31]Sternstein, Aliya and Moore, Jack. “Timeline: What we know about the OPM Breach (Updated).” NextGov. National Journal Group, 26 June 2015. Web. 21 Sep 2015.

[32]Sanger, David. “U.S. Decides to Retaliate Against China’s Hacking.” The New York Times. The New York Times Co., 31 Jul 2015. Web. 21 Sep 2015.

[33]Nakashima, Ellen and Warrick, Joby. “Stuxnet was work of U.S. and Israeli experts, officials say.” The Washington Post. The Washington Post, 2 June 2012. Web. 20 Sep 2015.

[34]F-Secure Labs Threat Intelligence. “The Dukes: 7 Years of Russian Espionage.” F-Secure, 16 Sep 2015. PDF.

[35]Healey, Jason and Hughes, Barry. “Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures.” Atlantic Council, 10 Sep 2015. PDF.

[36]Hern, Alex. “Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim.” The Guardian. Guardian News and Media Ltd., 6 Jul 2015. Web. 23 Sep 2015.

[37]Wilholt, Kyle. “The SCADA That Didn’t Cry Wolf.” Trend Micro Research Paper. Trend Micro, July 2013. PDF.

[38]McAfee Labs. “Quarterly Threat Report, August 2015.” Intel, 1 Sep 2015. PDF.

[39]Chen, Adrian. “The Agency.” The New York Times Magazine. The New York Times Co., 2 Jun 2015. Web. 21 Sep 2015.

[40]Sternstein, Aliya. “Russia Uses Army of ‘Trolls’ to Sway Sentiment Online.” National Journal. Atlantic Media, 17 Aug 2015. Web. 28 Sep 2015.

[41]Rogers, Michael S., Adm. “Cyber Operations: Improving the Military Cyber Security Posture in an Uncertain Threat Environment.” Testimony in front of the U.S. House Armed Services Committee. 4 Mar 2015. Web. 29 Sep 2015.

www.iisp.gatech.edu

#GTCSS15

Georgia Tech Institute for Information Security & Privacy