MIT Technology Review
BUSINESS REPORT

CONTENTS

Cyber Survival

With cyberattacks getting worse, the urgent need today is for faster responses, smarter technologies, and wider encryption.

SACHIN TENG

PLUS Europe Raises Data Walls | Tracking Cybercrime's Costs | Why Back Doors Worsen Cybersecurity | Priming Cyberinsurance Markets

The Big Question

Cybersecurity: The Age of the Megabreach

We haven't stopped huge breaches. The focus now is on resilience, with smarter ways to detect attacks and faster ways to respond to them.

● In November 2014, an especially chilling cyberattack shook the corporate world—something that went far beyond garden-variety theft of credit card numbers from a big-box store. Hackers, having explored the internal servers of Sony Pictures Entertainment, captured internal financial reports, top executives' embarrassing e-mails, private employee health data, and even unreleased movies and scripts and dumped them on the open Web. The offenders were said by U.S. law enforcement to be working at the behest of the North Korean regime, offended by a farcical movie the company had made in which a TV producer is caught up in a scheme to kill the country's dictator.

The results showed how profoundly flat-footed this major corporation was. The hack had been going on for months without being detected. Data vital to the company's business was not encrypted. The standard defensive technologies had not worked against what was presumed to have been a "phishing" attack in which an employee clicked a link that downloaded powerful malware. Taken together, all this showed that many of today's technologies are not adequate, that attacks can now be more aggressive than ever, and that once breaches occur, they are made worse by slow responses.

The Sony hack was one in a series of recent data breaches—including many "megabreaches," in which at least 10 million records are lost—that together reveal the weakness of today's cybersecurity approaches and the widening implications for the global economy. In 2015, the U.S. Office of Personnel Management was hacked, exposing 21.5 million records, including background checks on millions of people—among them copies of 5.6 million sets of fingerprints. Later in the year, 37 million visitors to Ashley Madison, a dating site for people seeking extramarital affairs, learned that their real e-mail addresses and other data had been released. The theft of data from 83 million customers of Wall Street giant J.P. Morgan, allegedly by an Israel-based team trying to manipulate the stock market, revealed chilling possibilities for how cyberattacks could undermine the financial sector.

Since companies and other organizations can't stop attacks and are often reliant on fundamentally insecure networks and technologies, the big question for this report is how they can effectively respond to attacks and limit the damage—and adopt smarter defensive strategies in the future. New approaches and new

Cyber Breaches Hit Staggering Levels

Exceptionally harmful hacks have recently struck organizations in the global insurance, finance, telecom, and entertainment industries and at the heart of a U.S. federal agency—inflicting hundreds of millions of dollars in damage and added costs.

		How They Were Exploited	Data Stolen and Scale	Costs	Suspected Culprit
7/2014	**JPMORGAN CHASE** New York City	Two-factor authentication upgrade not fully implemented.	Names, addresses, and phone numbers of 76 million household and seven million small-business accounts.	The company says it plans to spend $250 million annually on security.	Three people have been charged with the attack as part of a stock manipulation scheme.
11/2014	**SONY PICTURES ENTERTAINMENT** Culver City, California	Malware and lack of intrusion detection.	E-mails, salary information, and terabytes of other data, including movie scripts and contracts.	$41 million, according to public filings.	North Korean regime.
2/2015	**ANTHEM HEALTH** Indianapolis	Malware specifically designed to attack the company.	Names, birth dates, addresses, employment information, and Social Security numbers for 78 million people.	Much or all of the $100 million value of its cyberinsurance policy.	China-based hackers, suspected to be affiliated with the government.
6/2015	**U.S. OFFICE OF PERSONNEL MANAGEMENT** Washington, D.C.	Likely social-engineering attacks and lack of modern intrusion detection services.	A mix of names, birth dates, addresses, fingerprints, and background information on as many as 21.5 million people.	More than $133 million just for credit monitoring for victims.	China-based hackers, suspected to be affiliated with the government.
7/2015	**ASHLEY MADISON** Toronto	Unknown, but attackers cited weak passwords and almost nonexistent internal security.	Names, addresses, birth dates, phone numbers, and credit card history of 37 million users, plus the CEO's e-mails.	Unknown. The company faces numerous lawsuits.	A previously unknown group that calls itself Impact Team.
9/2015	**T-MOBILE US** Bellevue, Washington	Security weaknesses at a partner (Experian) that was managing credit check data.	Names, birth dates, addresses, and Social Security and driver's license numbers of 15 million people.	Experian has spent at least $20 million on credit monitoring and other corrective actions.	Unknown.
10/2015	**TALKTALK TELECOM** London	Distributed-denial-of-service attack and malicious code.	Names, birth dates, addresses, and phone numbers of more than 150,000 customers.	About $50 million in lost sales and incident response costs.	A teenager in Northern Ireland.

DATA SOURCES: SEC FILINGS, COMPANY STATEMENTS, EXPERIAN, NEW YORK TIMES, INSURANCE INSIDER

ways of thinking about cybersecurity are beginning to take hold. Organizations are getting better at detecting fraud and other attacks by using algorithms to mine historical information in real time. They are responding far more quickly, using platforms that alert security staff to what is happening and quickly help them take action. And new tools are emerging from a blossoming ecosystem of cybersecurity startups, financed by surging venture capital investment in the area.

But hindering progress everywhere is the general lack of encryption on the devices and messaging systems that hundreds of millions of people now use. Nearly three years ago, when National Security Agency contractor Edward Snowden revealed that intelligence agencies were freely availing themselves of data stored by the major Internet companies, many of those companies promised to do more to encrypt data. They started using encryption on their own corporate servers, but most users remain exposed unless they know to install and use third-party apps that encrypt their data.

$3.79 million
Average cost of a data breach

All these measures will help protect data in today's relatively insecure networks. But it's clear that the very basics of how networked technologies are built need to be rethought and security given a central role. A new national cybersecurity strategy is expected to chart an R&D plan to make sure software is verifiably secure and that users know when it's not working.

There's a big opportunity: the number of Internet-connected devices—not including smartphones, PCs, and tablets—could reach two billion in just five years. A 2015 McKinsey report predicts that this will become a multitrillion-dollar industry by 2025. All these new devices will present an opportunity to build things robustly from the start—and avoid having them play a role in Sony-like hacks in the future. *—David Talbot*

DATA SOURCE: SURVEY BY PONEMON INSTITUTE AND IBM; ILLUSTRATION: ROBERT RISKO

Expert Q&A

Why We're So Vulnerable

An expert in U.S. national cybersecurity research and policy says the next generation of technology must have security built in from the very start.

● In an age of continuing electronic breaches and rising geopolitical tensions over cyber-espionage, the White House is working on a national cybersecurity strategy that's expected in early 2016. Helping to draft that strategy is Greg Shannon. He was until recently chief scientist at Carnegie Mellon University's Software Engineering Institute and is now on leave to serve as assistant director for cybersecurity strategy at the White House Office of Science and Technology Policy.

In an interview with *MIT Technology Review* senior writer David Talbot, Shannon explained that dealing with today's frequent breaches and espionage threats—which have affected federal agencies as well as businesses and individuals—requires fundamentally new approaches to creating all kinds of software. Fixing the infrastructure for good may take two decades.

Cybersecurity has long been a serious worry. Have recent events really changed the game?

If you just consider the attack on Sony—it was a watershed event. The scale, scope, and cost were enormous. And it revealed how tightly cybersecurity and our economy are interrelated—and that the health of the economy is now potentially at stake.

Why are huge breaches like these happening? Are the billions of dollars spent on new security technologies in recent years not working?

It's more that the incentives to wage malicious cyber activities keep skyrocketing. In the early years of the Internet, the improved efficiencies from networked IT infrastructure far outweighed the security risks created by this infrastructure. Threats were always there, but it was okay to use patches. Today what's available online, and its value, keep increasing exponentially—and so do the incentives to exploit systems and steal data. What we are seeing are the results; absolutely, the threats and the attacks are bigger than they've ever been. And this hasn't been foremost in the mind-set of most companies producing software infrastructure or Internet services.

What is the underlying technology problem?

The answer might sound abstract and dry, but it has to do with efficacy and efficiency. On efficacy, how do you know that installing a new security technology is better than doing nothing? You often don't. And on efficiency, the usual approach is that you fix a newly discovered problem so the adversary doesn't use that method anymore. But at the end of the day this doesn't achieve much, because it doesn't create a general, systemic solution. It's not efficient.

We need to restructure how we build software, and develop security systems that have evidence that they actually add value. This requires rigor in how the billions of lines of code that run our networked infrastructure are actually written and updated.

The only places where software writing is truly rigorous are places like NASA—where they are building code that must work for years and from millions of miles away. They have highly formal methods and use well-controlled tools

and special engineering to make absolutely sure that the software is reliable and bug-free.

How can we make all IT infrastructure as great as the code running a Martian probe?
Many colleagues and I are devoted to this question. First, it's important to understand that there are a number of nontechnical issues that keep everyday software from being anywhere near that good. There aren't regulations or consequences that software companies experience if there are problems down the road—with the exception of certain high-priority domains like nuclear power plants or air traffic control.

So on the policy side you need to consider incentives for everybody to write better code—it could be because of liability, regulations, or market mechanisms. And on the technology side you need to create market incentives so rigorous software development methods, like the ones NASA uses, become far more efficient and easier for everyone to use. Congress, in the 2014 Cyber Security Enhancement Act, asked for a federal cybersecurity R&D strategic plan, and that plan is being drafted, for release by early 2016.

And while it will always be true that malicious insiders or human error can create problems, great software can to a large extent deal with that, too, by creating clear access rules and sending alerts when anything anomalous happens.

Meanwhile, what can companies do to protect themselves?
Every company, from the smallest to largest, should use best practices, taking into account each company's particular assets, threats, and cybersecurity capabilities. To be sure, many systems are inherently weak. Most systems have millions of lines of code, and the typical rate for a software bug is one per 1,000 lines of code. Even if one out of a hundred of these bugs winds up creating a security vulnerability, that's a density you can't really keep up with. But if companies follow best practices, they can become much better protected—and eventually avoid more [hacks like the one on] Sony.

We aren't getting NASA-level software, but is anyone doing it right?
One simple measure that is clearly critically necessary is that products need a way to have regular and secure software updates. One can argue that companies such as Tesla and Google and Apple—and, to a large extent, Microsoft—are doing that. Google Chrome updates happen in the background; it doesn't even ask you for permission anymore.

The emergence of an Internet of things—interconnecting billions of devices—provides an opportunity to do things correctly from the start.

The Apple iOS infrastructure does a good job of not requiring everyday app developers to worry about many, but not all, security issues. With Tesla, updates can happen when you charge the car.

What's the biggest opportunity right now to shape a more secure future?
The emergence of an Internet of things—interconnecting billions of devices—provides an opportunity to do things correctly from the start. Networked devices in cars and homes, and wearable devices, could introduce a multitude of new attack vectors, but if we get things right with these devices and cloud-based technologies, we can make sure the next generation of technology will have security built in.

How long until the efforts you've been talking about will make our networked infrastructure able to withstand the heightened incentives to attack it?
For the most critical components in areas like the electric grid and large industrial systems, five to 10 years is feasible. To be pervasive it will take 20 or more years.

Venture Capital

Venture Capitalists Chase Rising Cybersecurity Spending

Investors have been pouring money into companies selling "next-generation" security products.

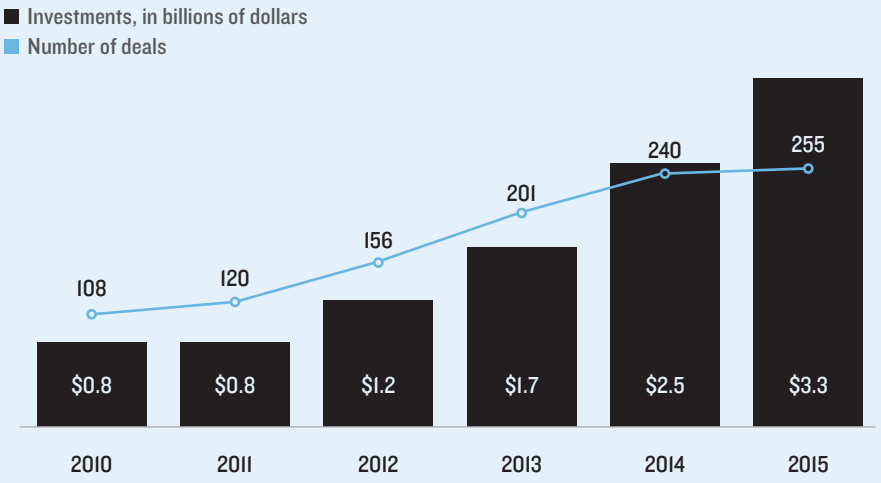
● The rash of headline-grabbing cyberattacks on major companies over the past few years has made one thing abundantly clear: it's not enough to rely only on traditional security tools. To venture capitalists, that means there's money to be made by betting on startups developing new ones.

VCs are hoping to get a piece of companies' increased spending on cybersecurity. In 2014 Gregg Steinhafel, the CEO of Target, became the first head of a major company to lose his job over a data breach. Now, worried company leaders are giving their security units a "blank check," says Scott Weiss, a general partner who specializes in security at the venture capital firm Andreessen Horowitz: "The CEO has said, 'Look, whatever you need, you've got.'"

$3.3 billion
2015 VC investment in cybersecurity

Today's advanced threats are much too sophisticated for traditional tools like antivirus software and firewalls. Not wanting to buy obsolete products, security executives are increasingly venturing into agreements with cybersecurity startups. To Weiss and other venture investors, that kind of customer demand is an investment opportunity. According to CB Insights, the global VC community

Rising Venture Capital Interest in Cybersecurity Startups



poured a record $2.5 billion into cybersecurity companies in 2014, a strong year for IT startups in general and software in particular. Security companies raised another $3.3 billion in 2015.

The problems these startups are trying to solve are complex. The bad guys do have better weapons, but business systems are also becoming vulnerable in new ways. Businesses are relying more on cloud services and connecting more "things" to the Internet, and their employees are using more connected devices.

Before a few years ago, the conventional approach to security entailed basically building a wall around valuable data and using software to detect known signatures of malicious code. Then security researchers began finding extremely complex malware, derived from government-designed exploits and sophisticated enough to circumvent traditional antivirus tools. This new generation of malware can be custom-built for a specific network and more precisely controlled by its human operators.

Dealing with such specialized, fast-evolving adversaries requires changing the security paradigm from prevention to "active cyberdefense," says Nicole Eagan, CEO of Darktrace, a two-year-old company based in Cambridge, United Kingdom. Hackers are going to get in, so the trick now is to find them "in near real time as they are moving subtly and silently around your network" and catch them before they do any real damage, she says.

Many of the new startups are focused on trying to detect hackers in real time as they enter and move subtly through a corporate network.

A number of companies, taking a range of different approaches, promise that their detection technologies can do this. Darktrace, which has raised $110 million in VC funding, relies on advanced machine-learning technology to analyze raw network traffic and, as Eagan explains, "determine a baseline for what's normal" for every person using the network so that it can detect abnormal behavior.

Not only are the threats more numerous and advanced, but companies must also secure networks that are growing more complex and massive. Every device on a network is a potential target for hackers, and new security technologies focused on them are getting lots of attention from investors.

A company called Tanium, which is now valued at $3.5 billion after its most recent round of VC investment, has technology that allows network operators to ask questions about what's happening in any one of millions of devices on a network. They get an answer within 15 seconds and can quickly take action—for example, by quarantining an infected computer.

Security investors are also focused on the fact that businesses and organizations are putting more and more data in the cloud. In response to this trend, a new breed of cloud security companies are offering services such as novel encryption schemes and technologies for continuously monitoring what goes on in a company's cloud servers.

With so much funding available, the burgeoning cybersecurity startup scene is chaotic. Greg Dracon, a partner at .406 Ventures who has invested in several security companies, thinks a consolidation cycle may already be starting. Bigger companies are buying up individual technologies and could eventually offer suites of products, he says.

Dracon thinks all this investor attention is driving prices too high overall, and that the market has gotten ahead of itself, at least for the near term. However, the security market itself has another decade of growth at least, he believes. "The problem set is outpacing the solution set," he says, "and I don't think there's any end in sight to that." —*Mike Orcutt*

DATA SOURCE: CB INSIGHTS

Case Study

How PayPal Boosts Security with Artificial Intelligence

The payments giant keeps fraud losses below industry averages by teaching computers to play detective.

● To PayPal, the transactions signal fraud: a U.S. user's account is accessed in the U.K., China, and elsewhere around the world. But PayPal's security

system—thanks to a growing reliance on an artificial-intelligence technology known as deep learning—is now able to spot possible fraud without making mistakes. That's because algorithms mine data from the customer's purchasing history—in addition to reviewing patterns of likely fraud stored in its databases—and can tell whether, for example, the suspect transactions were innocent actions of a globe-hopping pilot.

From a cybersecurity perspective, PayPal has a target on its back: it processed $235 billion in payments last year from four billion transactions by its more than 170 million customers. Fraud is always possible via theft of consumer data in breaches such as "phishing" e-mails that con users into entering their credentials. To keep ahead, PayPal relies on intensive, real-time analysis of transactions.

When a pattern is revealed—for example, if sudden strings of many small purchases at convenience stores turn out to be fraud—it's turned into a "feature," or a rule that can be applied in real time to stop purchases that fit this profile. "We now process thousands of 'features' in our system, compared to hundreds when the system was first put to use in 2013," says Hui Wang, the company's senior director of global risk sciences.

As a result, PayPal can now do things like tell the difference between friends buying concert tickets together and a thief making similar purchases with a list of stolen accounts. And it's all done in-house to avoid even the tiny latency that would occur if the company relied on a cloud provider. "Thousands of 'features' searching through 16 years of users' history all needs to be done in less than a second," Wang says.

As a transaction is being made, PayPal's deep-learning algorithms can search 16 years of user purchasing history and thousands of fraud patterns to spot theft while avoiding error.

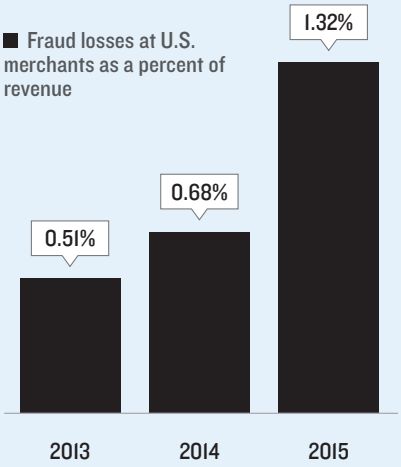
Deep learning and other artificial-intelligence approaches are quickly becoming the only way to keep up with threats, she adds. They've worked to help keep PayPal's fraud rate remarkably low, at 0.32 percent of revenue—a figure far better than the 1.32 percent average that merchants see, according to a study by LexisNexis. The most recent Federal Reserve Payments Study found that $6.1 billion in fraudulent purchases were made in 2012, and the problem appears to be getting worse.

PayPal isn't the only company using deep learning to improve cybersecurity. The Israeli startup Deep Instinct has employed the technique to spot malware, claiming that this works 20 percent better than traditional approaches. And Ashar Aziz, vice chairman and founder of the security firm FireEye, said that his company has been using deep learning for everything from detecting network intrusions to rooting out phishing attacks.

Companies can further improve cybersecurity if they share data repositories on cyberattacks and fraud, says Aziz. "If you continue to get more data—and more power to process it—then you can get even better," he says. —*Michael Morisy*

Rising Crime

Fraud losses are increasing. But PayPal's rate is only 0.32%.



DATA SOURCE: LEXISNEXIS TRUE COST OF FRAUD REPORT

Encryption

Half-Measures on Encryption Since Snowden

Amid a wave of corporate privacy and security pronouncements, 2014 was supposed to be the "year of encryption." It didn't pan out that way.

● When the NSA subcontractor Edward Snowden released classified documents in June 2013 baring the U.S. intelligence community's global surveillance programs, it revealed the lax attention to privacy and data security at major Internet companies like Apple, Google, Yahoo, and Microsoft. Warrantless surveillance was possible because data was unencrypted as it flowed between internal company data centers and service providers.

The revelations damaged technology companies' relationships with businesses and consumers. Various estimates pegged the impact at between $35 billion and $180 billion as foreign business customers canceled service contracts with U.S. cloud computing companies in favor of foreign competitors, and as the companies poured money into PR campaigns to reassure their remaining customers.

There was a silver lining: the revelations catalyzed a movement among technology companies to use encryption to protect users' data from spying and theft. But the results have been mixed. Major service providers including Google, Yahoo, and Microsoft—who are among the largest providers of cloud- and Web-based services like e-mail, search, storage, and messaging—have indeed encrypted user data flowing across their internal infrastructure. But the same isn't true in other contexts, such as when data is stored on smartphones or moving across networks in hugely popular messaging apps like Skype and Google Hangouts. Apple is leading the pack: it encrypts data by default on iPhones and other devices

running newer versions of its operating system, and it encrypts communications data so that only the sender and receiver have access to it.

But Apple products aren't widely used in the poor world. Of the 3.4 billion smartphones in use worldwide, more than 80 percent run Google's Android operating system. Many are low-end phones with less built-in protection than iPhones. This has produced a "digital security divide," says Chris Soghoian, principal technologist at the American Civil Liberties Union. "The phone used by the rich is encrypted by default and cannot be surveilled, and the phone used by most people in the global south and the poor and disadvantaged in America can be surveilled," he said at *MIT Technology Review*'s EmTech conference in November.

Pronouncements on new encryption plans quickly followed the Snowden revelations. In November 2013, Yahoo announced that it intended to encrypt data flowing between its data centers and said it would also encrypt traffic moving between a user's device and its servers (as signaled by the address prefix HTTPS). Microsoft announced in November and December 2013 that it would expand encryption to many of its major products and services, meaning data would be encrypted in transit and on Microsoft's servers. Google announced in March 2014 that connections to Gmail would use HTTPS and that it would encrypt e-mails sent to other providers who can also support encryption, such as Yahoo. And finally, in 2013 and 2014, Apple implemented the most dramatic changes of all, announcing that the latest version of iOS, the operating system that runs on all iPhones and iPads, would include built-in end-to-end encrypted text and video messaging. Importantly, Apple also announced it would store the keys to decrypt this information only on users' phones, not on Apple's servers—making it far more difficult for a hacker, an insider at Apple, or even government officials with a court order to gain access.

Google, Microsoft, and Yahoo don't provide such end-to-end encryption of communications data. But users can turn to a rising crop of free third-party apps, like ChatSecure and Signal, that support such encryption and open their source code for review. Relatively few users take the extra step to learn about and use these tools. Still, secure messaging apps may play a key role in making it easier to implement wider encryption across the Internet, says Stephen Farrell, a computer scientist at Trinity College Dublin and a leader of security efforts at the Internet Engineering Task Force, which develops fundamental Internet protocols. "Large messaging providers need to get experience with deployment of end-to-end secure messaging and then return to the standards process with that experience," he says. "That is what will be needed to really address the Internet-scale messaging security problem." —*David O'Brien*

Sobering Message

Unlike other big players, Apple does a thorough job of encrypting messages.

	Encrypted in transit	Encrypted end-to-end	Supports verification of contacts' identities	Deletes encryption keys after use	Code open to independent review	Properly documents security	Recently audited
iMESSAGE (APPLE)	●	●		●		●	●
FACETIME (APPLE)	●	●		●		●	●
HANGOUTS/CHAT (GOOGLE)	●						●
SKYPE (MICROSOFT)	●						
YAHOO MESSENGER	●						

ILLUSTRATION: PATRICK KYLE; DATA SOURCE: ELECTRONIC FRONTIER FOUNDATION

Incident Response

New Rapid Response Systems Blunt Cyberattacks

Limiting damage from attacks requires far faster reactions, quick notification of victims, and adherence to regulations. Managing all that can be tricky.

● One reason breaches do so much damage is that they often remain undiscovered for months—an average of more than 200 days, according to research by the security firm Mandiant. Over time, a once-minor breach can become a catastrophe.

Sometimes the intrusion is hard to spot because the hacker has stolen legitimate credentials. Other times subtle hints of unusual network activity that might have revealed the attack are simply missed.

When such clues go unnoticed, it is often because large corporate security systems are so complex. It's not unusual for a big company to use 70 or more different security monitoring tools made by many different companies and adopted over time—intrusion detectors, firewalls, Web-page monitors, spam filters, and many others. This common situation "is a huge problem," says Jon Oltsik, cofounder of Enterprise Strategy Group, an IT research firm. "It depends on very, very smart people to figure out what each system is telling them and put together the total picture."

One solution is for companies to replace whatever they've already installed with integrated systems from giant vendors like IBM, Cisco, and Raytheon. But that can be expensive and impractical for many.

So a growing crop of startups and research projects are beginning to offer approaches aimed at making it easier to tie existing systems together, while also making it possible to respond to attacks quickly and appropriately.

One early entrant, Resilient Systems, a startup in Cambridge, Massachusetts, captures data from a variety of sources and provides a single dashboard displaying all warnings. Then it presents a checklist of actions that must be taken, both to fix the problem and also to do things like notify the U.S. Federal Trade Commission or comply with state-by-state consumer notification laws. *—David Talbot*

Incident Response: An Emerging Field

Startup companies are joining major federal research efforts and open-source technologies to create quick and effective responses to cyberattacks.

	Technology	Date
RESILIENT SYSTEMS Cambridge, MA	Cyberattack detection and response platform	Launched in 2011
INVOTAS Alexandria, VA	Cyberattack detection and response platform	Launched in 2014
HEXADITE Tel Aviv, Israel	Cyberattack detection and response platform	Launched in 2014
NETFLIX Los Gatos, CA	Open-source software for cyberattack detection and response	Released in 2015
U.S. DEPARTMENT OF DEFENSE/JOHNS HOPKINS UNIVERSITY	Adaptable cyber response systems	Ongoing federal research project
U.S. DEPARTMENT OF HOMELAND SECURITY	Automated cybersecurity for businesses	Recent government/industry collaboration

Emerging Technologies

Finding Insecurity in the Internet of Things

The world of connected devices is growing fast, but how secure is it?

● As we connect everything from Barbie dolls to front-door locks and cars to the Internet, we're creating more—and possibly more dangerous—potential ways for cyberattackers to wreak havoc.

Security researchers have reported on the ease with which you can break into a range of connected gadgets like baby monitors and cars. This past summer a piece in *Wired* showed how a software bug could be exploited to control a Jeep driving down the highway. (Jeep owner Chrysler quickly fixed the bug.)

21 billion
Number of Internet-connected "things" expected in 2020

Mika Ståhlberg, director of strategic threat research at the Finnish security company F-Secure, points out that while a hacked credit card may be a headache, a hacked smart lock could open your home to burglars.

A number of startups have started offering security for the Internet of things. In November, F-Secure announced a product called Sense that can monitor Internet-connected devices like smartphones, smart lights, and baby monitors. The device, which should be available in the spring, keeps an eye on network metadata—which includes information like where data is going or coming from, and how much is being sent overall—and blocks activity thought to be malicious. Atlanta-based Bastille, meanwhile, uses

DATA SOURCE: SYMANTEC

sensors to keep track of connected devices by measuring the electromagnetic signatures of different devices in an office. The sensors can track devices that use communication protocols like Wi-Fi and low-energy Bluetooth or work over cellular networks, and its software can tell where they are to within three meters. Bastille's tactic of scanning a wide spectrum of radio frequencies suits Internet-connected gadgets since they are designed using many different protocols.

The potential range of attack targets is rising: Gartner, the market research firm, predicts that by 2020, almost 21 billion gadgets will be connected to the Internet, up from 4.9 billion today. "This is the World Wide Web of 1994, 1995. We know it's going to be big," says Phil Levis, an associate professor at Stanford who co-directs the university's Secure Internet of Things Project. "It's going to be a security train wreck, much as the Web was for 10 years or so until people figured it out."

Levis isn't convinced monitoring is the best approach, because behavior variations will only show up after a device has been compromised or an attack has occurred, he says. What really needs to happen, he says, is for device manufacturers to write secure software in the first place. The Internet is in some ways more secure now than two decades ago, because developers are more careful and clean up dangerous code. These lessons have yet to be picked up by many Internet-of-things developers, he says. *—Rachel Metz*

China

China Hit by Rise of Attacks

China sees a major increase in infections on file-sharing sites and more targeted, localized malware threats.

● China-based hackers are sometimes accused of being behind major external attacks like the one on the U.S. Office of Personnel Management, as well as acts of corporate espionage. But China has worsening internal problems, too.

In September, a counterfeit copy of Apple's Xcode software development tool was offered on a local file-sharing site, leading to infections on iPhone apps created with the fake tool. The hack, which ended up affecting more than 100 million mostly China-based iPhone users, was Apple's biggest security breach to date.

A possibly even larger hack was an October attack on NetEase, one of the top social-media and news platforms in China. A hack of its 163.com e-mail system, which is still under investigation, potentially exposed the aliases, security questions and answers, passwords, and other data of hundreds of millions of primarily Chinese users.

Hong Jia, a cofounder of the China-based threat intelligence firm ThreatBook and former cybersecurity expert at Microsoft, says companies and individuals in China are beginning to wake up to the threat. "Enterprises [in China] know that someday they will get targeted and a whole company can be exposed by an attack," Hong said in an interview at the Association of Anti-Virus Asia Researchers International Conference, held in December in Danang, Vietnam.

According to a survey by auditing firm PricewaterhouseCoopers, over the past year companies in China and Hong Kong saw around 1,245 attacks each on average, compared with 241 the year before. In addition to big hacks like the iPhone incident, Chinese companies have experienced a rapidly rising number of attacks that use so-called social engineering to trick individuals into clicking links that download malware onto the user's computer. "The threats you see in China are really, really targeted," Ingvar Froiland, director and general manager for the security company F-Secure, said in an interview at the Danang conference. Froiland said the threats are often language-specific or event-specific—such as targeted attacks during Chinese New Year and other holidays. He added that they also may be system- and application-specific: for example, they are sometimes launched through games that may not be used widely outside China, or through file-sharing sites accessed mainly by Chinese users.

At Chinese companies, attacks are rising sharply. And Chinese hackers are launching more internal attacks through local file-sharing sites and games used mainly within the country.

Chinese authorities even discovered a "hacking village" last year. In a mostly rural area bordering Vietnam, large numbers of people were involved in cybercrime, cyberfraud, and hacking, often using the popular QQ instant messaging software run by Tencent, one of the world's biggest Internet companies.

At the Danang conference, Liu Zhao, an antimalware analyst at Tencent, said he has been finding increasing numbers of new tricks deployed by hackers in China, including malicious files masquerading as harmless icons attached to documents sent to specific victims. Real-world parent-teacher, school-student, or business-consumer relationships—often discovered from stolen e-mails—are sometimes used for extortion, he added.

1,245
Average number of attacks on a Chinese company per year

To fight targeted attacks, Hong said, analysts are working on analyzing traffic flowing from computer addresses and domain names to find the source, such as the hacking village. "We can see ... what person might be behind it," Hong said. Adding to China's woes is that citizens often do not add protections to their mobile devices. Worldwide, "awareness of threats to mobile devices is not there yet," Froiland said. *—Michael Standaert*

Policy

Europe Raises Barriers to American Data Transfers

Citing Snowden, a European court throws into doubt whether many U.S. companies can easily haul European data across the Atlantic.

● In October the European Union's highest court invalidated the data protection agreement known as Safe Harbor, which had allowed 4,332 American companies to transfer the personal data of the European Union's 500 million citizens back and forth across the Atlantic.

The decision was a result of the 2013 revelations by NSA contractor Edward Snowden, which exposed the U.S. government's access to personal data on the servers of companies like Google and Microsoft. Now, U.S. companies are facing pressure to keep the data of European users in Europe. And in some cases Europeans may be left in the hands of lesser-known companies whose main selling point is that they're not holding data in the U.S.

There is little evidence that either trend will benefit cybersecurity, says Herbert Lin, a senior researcher at Stanford's Center for International Security and Cooperation. "I would argue that in general the American IT industry is significantly ahead of the rest of the world, and if you want the best technical talent applied, you go American," he says. He points out that intelligence agencies in the United Kingdom, Germany, and elsewhere in Europe were just as deeply implicated in the Snowden documents as their counterparts in the U.S. "Just because the data is hosted over there doesn't change the security dimensions of it very much," he adds.

Safe Harbor was established in 2000 as a way for American businesses operating in Europe to self-certify that they were in compliance with the stricter privacy protections afforded by law to European Union citizens, which include the right to access the personal data collected by companies, as well as the right to have that data deleted.

Prodded by the Snowden disclosures, the European court basically said it was no longer going to take American companies' word for any of this.

With the agreement now abolished, American companies had until the end of January to demonstrate some other mode of compliance. Companies face the nightmare of either reworking all their contracts to include clauses preapproved by European regulators or asking users to provide so-called "informed consent" to every data transfer. Both options are unwieldy for many businesses, says J. Trevor Hughes, president and CEO of the International Association of Privacy Professionals in Portsmouth, New Hampshire, and may make it impossible for them to operate in Europe.

4,332
Safe Harbor–certified companies

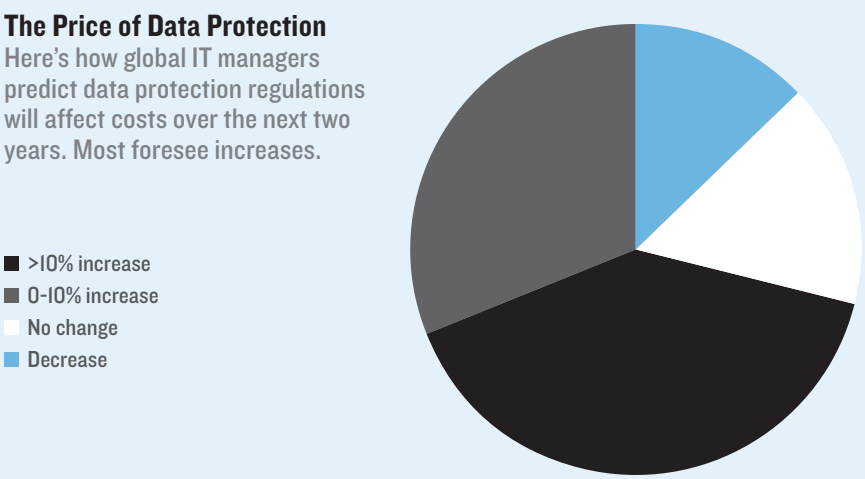
First Data, a company that processes 2,300 financial transactions per second for clients in 118 countries around the world, got ahead of the ruling by bringing in lawyers to help it secure approval for its data policies from regulators in the United Kingdom in a lengthy bottom-up review of the whole company. "We had to pull in as an organization all of our teams to be able to say we've got the right processes and procedures in place to protect data," says Christine Sevener, First Data's chief privacy officer.

Policy makers are trying to avoid a balkanized cybersecurity landscape in which companies would have to follow different rules every time they sent someone's data across a national border.

Others with enough cash to afford it are establishing special data centers abroad. In November, Microsoft announced that it would soon begin hosting the cloud data of E.U. citizens in Germany in partnership with a subsidiary of Deutsche Telekom. Not only does the move sidestep the issue of trans-Atlantic data transfers, but there is a clear business case to be made for it; Microsoft pointed to a study showing that 83 percent of German businesses expect their cloud provider to operate data centers locally.

Talks between U.S. and European policy makers are aimed at forging a new agreement. This will be critical to avoid-

The Price of Data Protection
Here's how global IT managers predict data protection regulations will affect costs over the next two years. Most foresee increases.



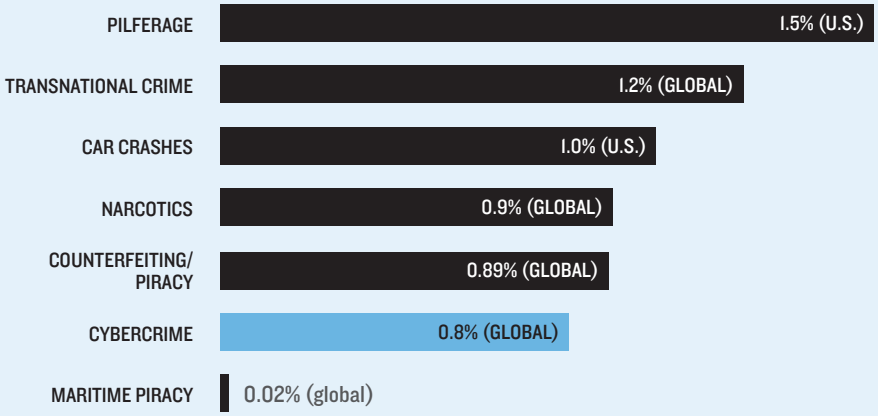
DATA SOURCE: OVUM

ing a balkanized cybersecurity landscape where companies have to deal with different rules and regulations whenever data moves across a national border.

Under the ruling, "each country in Europe is going to be responsible for determining on their own whether or not [data transfers] are valid," says Daniel Castro, vice president of the Information Technology and Innovation Foundation, a think tank based in Washington, D.C. "So it's not just that the court has raised the cost of compliance, but they've also multiplied it times all the different European Union member states." *—Matt Mahoney*

Ballpark Numbers on the Global Costs of Cybercrime

A 2014 analysis by the Center for Strategic and International Studies and Intel Security put the global cost of cybercrime at up to $575 billion annually, or 0.8 percent of global GDP. Here's how that GDP hit compares with that of other common sources of loss. Numbers refer to percent of GDP.



DATA SOURCE: INTEL SECURITY AND THE CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

Economics

No One Knows How Much Cybercrime Really Costs

A lack of reliable figures on the costs of many kinds of cybercrime is holding back companies and governments from responding appropriately.

● Before the Grum botnet of several hundred thousand compromised computers was taken down by law enforcement in 2012, it was responsible for sending out 18 billion spam messages per day, mostly hawking pharmaceuticals such as Viagra.

Grum was earning its operators nearly $3 million a year for pushing drug ads, but far more impressive were the indirect costs it imposed: it was believed responsible for nearly 20 percent of the world's spam, which researchers at Microsoft and Google say costs the world $20 billion a year on things like e-mail filtering and storage.

The case of Grum is unusual in that the finances of spam are relatively well understood, making it possible to do a cost-benefit analysis of actions taken to stop it. That's not the case with other threats, such as data breaches that feed personal information to the black market.

Although it's clear that cybercrime imposes real and sizable costs on society, fine-grained data is generally hard to come by.

"Many of the private-sector reports are basically marketing brochures from organizations with a strong interest in scaremongering," says Ross Anderson, a professor of security engineering at the University of Cambridge.

Law enforcement agencies lack good statistics on the incidence and costs of cybercrime because they have not updated their operations for the Internet era.

And law enforcement agencies and police don't have good statistics on the incidence and costs of cybercrime because they have not updated their operations for the Internet era as well as criminals have, he says. A European Union research project recently concluded that a lack of clear figures on costs was preventing companies as well as governments and law enforcement from making good decisions about security.

"If data is patchy or unverifiable, then it is likely that businesses will either waste money or not spend any at all, leaving themselves and consumers vulnerable to attack," says Jart Armin, a founder of the security company CyberDefcon, who is involved with the CyberROAD project behind the E.U. report.

Anderson and colleagues at Cambridge are in the process of setting up a new research center that could help clear up that confusion. The Cambridge Cloud Cybercrime Center will operate as a kind of clearinghouse for data from major companies—data that can be mined to discover the patterns of criminal activity. "We've got to be able to measure cybercrime to be effective in doing anything about it," says Anderson.

Talks are under way with Google, Yahoo, and others interested in donating data.

"For the first time we're going to be able to look at stuff at scale," says Anderson. He hopes that the new resource will produce insights into the patterns and costs of cybercrime that could allow far more informed responses. *—Tom Simonite*

DO YOU

BELIEVE ANTIVIRUS PROTECTS YOUR BUSINESS?

EVEN

ANTIVIRUS VENDORS DON'T THINK SO.

Let us show you a better way to protect your business.

SEE THE TRUTH >>

Viewpoint

How an Overreaction to Terrorism Can Hurt Cybersecurity

Encryption could have prevented some of the worst cyberattacks. Giving back doors to law enforcement will make matters worse, argues Bruce Schneier.

● Many technological security failures of today can be traced to failures of encryption. In 2014 and 2015, unnamed hackers—probably the Chinese government—stole 21.5 million personal files of U.S. government employees and others. They wouldn't have obtained this data if it had been encrypted.

Many large-scale criminal data thefts were made either easier or more damaging because data wasn't encrypted: Target, T.J. Maxx, Heartland Payment Systems, and so on. Many countries are eavesdropping on the unencrypted communications of their own citizens, looking for dissidents and other voices they want to silence.

Some law enforcement leaders have proposed adding back doors to encrypted data to allow access for court-authorized investigations, arguing that this will prevent criminals or terrorists from "going dark," as FBI director James Comey put it in a 2014 Brookings Institution talk ("Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?"). But that approach will only exacerbate the risks.

We can't build an access system that works only for people with a certain citizenship or a particular morality, or in the presence of a specified legal document. If the FBI can eavesdrop on your text messages or get at your computer's hard drive, so can other governments. So can criminals. So can terrorists. If you want to understand the details, read a 2015 paper coauthored by MIT professor Hal Abelson, called "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications."

If the FBI can eavesdrop on your text messages or get at your computer's hard drive, so can other governments. So can criminals. So can terrorists.

The debate over whether law enforcement should gain access to encrypted messages and other data reëmerged in light of the Paris terror attacks and others. But it's a false choice to say you can have either privacy or security. The real choice is between having less security and having more security. Of course, criminals and terrorists have used—are using, will use—encryption to hide their planning from the authorities, just as they will use society's amenities and infrastructure: cars, restaurants, telecommunications. In general, we recognize that such things can be used by both honest and dishonest people. Society thrives nonetheless, because the honest so outnumber the dishonest.

The security technologist Bruce Schneier is the author most recently of Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.

Markets

Can We Insure the Internet of Things Against Cyber Risk?

Software with security flaws, and a lack of historical data on risks, have made the Internet of things tough to insure.

● Insuring the security of connected products is hard for a simple reason: they are too new, and too little is known about the economic losses or personal injury they might cause. What the industry needs is data, and analytics to translate statistics on losses into policy standards and consistent pricing. Only then can emerging industries like self-driving cars and network-connected medical devices really take off, says software security expert Josh Corman.

Efforts to build a strong insurance industry in this area are expected to begin bearing fruit in early 2016, experts say. A number of groups have begun setting standards for protecting cybersecurity in Internet-of-things devices, and the hope is that they will standardize insurance practice and begin establishing the legal standards for handling data, helping to determine who's responsible for what losses when things go wrong, says George Washington University Law School lecturer Paul Rosenzweig.

Makers of next-generation connected devices—and services—need insurance against malfunctions from bad software as well as any damage hackers might cause. Many connected devices and the systems connecting them use freely available open-source software that has security flaws well known to the industry, says Corman.

TOMI UM

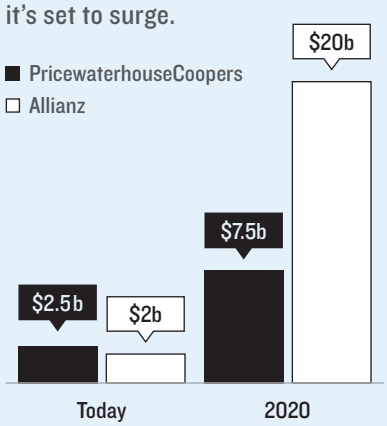
But even highly customized software can pose problems. Tesla's release last summer of an autonomous-steering upgrade illustrated the possible risk, though no injuries were reported. Hackers also demonstrated that they could remotely take over a Jeep through its onboard computers. The potential for cars to cause accidents shows how computer-security problems can cause trouble distinct from the harm done in traditional cybercrimes like theft of credit card data. As Internet business, once centered on retailing, becomes a hub for manufacturers, health care, and services, its insurance needs get more complicated.

Carriers have sold limited amounts of cyberinsurance for years, but little is known about the market, says Eric Nordman, director of regulatory services at the National Association of Insurance Commissioners, a group of state regulators. Almost all the insurance written now is believed to cover the costs of losing customers' personal information to hackers. State laws require disclosure of those breaches, so carriers know how common the incidents really are, and how much they cost to fix. Loss of intellectual property or personal injury, such as injuries that might occur if Tesla's steering system were hacked, are often simply not insurable, Rosenzweig says.

—Tim Mullaney

Boom Times for Cyberinsurance

Experts differ on the size of the cyberinsurance market but agree it's set to surge.



Outside Reading

"Avoiding the Top Ten Software Security Design Flaws"

By Iván Arce et al.
The IEEE Center for Secure Design, August 2014

Part of the IEEE's Cybersecurity Initiative, this handbook features some of the leaders in academia and industry identifying the most common areas of vulnerability for software in an effort to promote stronger, more resilient systems.

The authors point out that a great deal of effort in information security is devoted to finding implementation bugs, rather than recognizing and correcting fundamental flaws in design. The 10 sections address topics such as user authentication, the separation between code and data, comprehensive data validation, and the proper use of cryptography, providing tips and describing best practices.

Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It

By Marc Goodman
Doubleday, February 2015

In his new book, Marc Goodman, an investigator and security advisor who has worked with Interpol, the United Nations, NATO, and the LAPD, details how throughout history organized criminal and terrorist enterprises have consistently been the earliest adopters of new technologies, leaving police, politicians, and the rest of us always a few steps behind. In today's interconnected world, it has never been easier for tech-savvy criminals to attack vulnerable organizations and individuals, often without needing to move from behind their computer screens halfway around the world from their victims. And just as law enforcement begins to infiltrate hacker networks and online terrors cells, the author warns, these individuals are already learning to exploit next-generation technologies like robotics, virtual reality, 3-D printing, and synthetic biology.

Executive Order Promoting Private Sector Cybersecurity Information Sharing

By Barack Obama
February 2015

In the wake of the cyberattack against Sony Pictures that crippled the studio in November 2014, President Obama issued an executive order calling for greater coöperation in sharing information about cybersecurity risks, both within the private sector and between industry and government. At the first White House summit on Cybersecurity and Consumer Protection, held at Stanford University in February to coincide with the issuing of the order, Obama said, "There's only one way to defend America from these cyber threats, and that is through government and industry working together, sharing appropriate information as true partners."

"A 'Building Code' for Internet of Things Security, Privacy"

By Greg Shannon
InformationWeek's DarkReading.com, March 2015

This post from the chief scientist for the CERT(r) Division at Carnegie Mellon University's Software Engineering Institute argues for the development of new standards to make wearable and implanted medical devices as secure as possible from interference and snooping. Shannon argues that because these devices are often small and low on power, with limited processing capabilities, they present some unique challenges in preventing cyberattacks. Another problem involves devices that, with FDA approval, can continue to be used regardless of security vulnerabilities.

Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World

By Bruce Schneier
W.W. Norton, March 2015

Bruce Schneier surveys the terrain in the post-Snowden world in his provocative new book. After giving numerous examples of just how much personal information businesses and governments can collect about us from our mobile phones and our social-network posts, and the uses and misuses to which that data can be put, he offers a road map to reform. While most readers will accept that lines have to be drawn somewhere, Schneier's proposal that companies with access to vast databases of personal information should face heavy government regulation may be a harder sell.

"Cyber-Espionage Nightmare"

By David Talbot
MIT Technology Review, July/August 2015

MIT Technology Review's senior writer gives the story behind last spring's federal indictment of five Chinese military hackers accused of economic espionage against six U.S. companies, including Westinghouse, U.S. Steel, and Alcoa. It was the first such case brought against the perpetrators of state-sponsored cyber-espionage, and the article explores how it has affected relations between the two countries and brought into the open the sort of computer security vulnerabilities that private companies rarely acknowledge in public.

"How to Implement Security after a Cyber Security Meltdown"

By Christina Kubecka
Black Hat USA, August 2015

In one of the most anticipated talks at last year's Black Hat security conference, information security consultant Christina Kubecka offered an inside perspective on how one company dealt with one of the largest cyberattacks in history. During Ramadan 2012, an unknown group of hackers calling themselves the "Sword of Justice" released a virus into the computer networks of Saudi Aramco, the world's largest oil company, wiping out the data on over 30,000 workstations. The swiftness and vast scale of the attack forced the state-run company to go completely offline to contain the threat and rebuild most of its IT infrastructure from the ground up.

"Securing Today's Data Against Tomorrow's Quantum Computers"

By Tom Simonite
TechnologyReview.com, August 3, 2015

Ever since 1994, when Peter Shor developed a quantum algorithm that could break the form of encryption most commonly used to protect data online, security experts have known that new protocols would be needed once scalable quantum computers became a reality. For a long time this has been seen as a distant prospect, but this article from *MIT Technology Review*'s San Francisco bureau chief shows how Microsoft is getting a head start. A research project there succeeded in upgrading the encryption protocol that secures the Web so that it's able to resist quantum attacks.

"A Riddle Wrapped in an Enigma"

By Neal Koblitz and Alfred J. Menezes
International Association for Cryptologic Research, October 2015

In August 2015, the National Security Agency published an update online of its plans for moving to quantum-resistant algorithms. While the mere fact that the primary U.S. spy agency saw the arrival of practical quantum computing as imminent made headlines, the NSA also tipped its hand that a type of quantum-resistant algorithm it had once championed, known as elliptic curve cryptography, "is not the long-term solution many once hoped it would be." This paper from two well-respected academic cryptographers speculates about what this about-face means and whether the NSA knows something about these widely used algorithms that the cryptography community doesn't.

Calendar

SANS Cyber Threat Intelligence Summit
February 3–10, 2016
Alexandria, Virginia
www.sans.org/event/cyber-threat-intelligence-summit-2016

RSA Conference
February 29–March 4, 2016
San Francisco
www.rsaconference.com/events/us16

Black Hat Asia
March 29–April 1, 2016
Singapore
www.blackhat.com/asia-16

IAPP Global Privacy Summit
April 3–6, 2016
Washington, D.C.
https://iapp.org/conference/global-privacy-summit-2016

InfoSec World
April 4–6, 2016
Lake Buena Vista, Florida
http://infosecworld.misti.com

IEEE Symposium on Security and Privacy
May 23–25, 2016
San Jose, California
www.ieee-security.org/TC/SP2016

Infosecurity Europe
June 7–9, 2016
London
www.infosecurityeurope.com

Black Hat USA
July 30–August 4, 2016
Las Vegas
www.blackhat.com

DEF CON
August 4–7, 2016
Las Vegas
www.defcon.org

USENIX Security Symposium
August 10–12, 2016
Austin, Texas
www.usenix.org/conference/usenixsecurity16