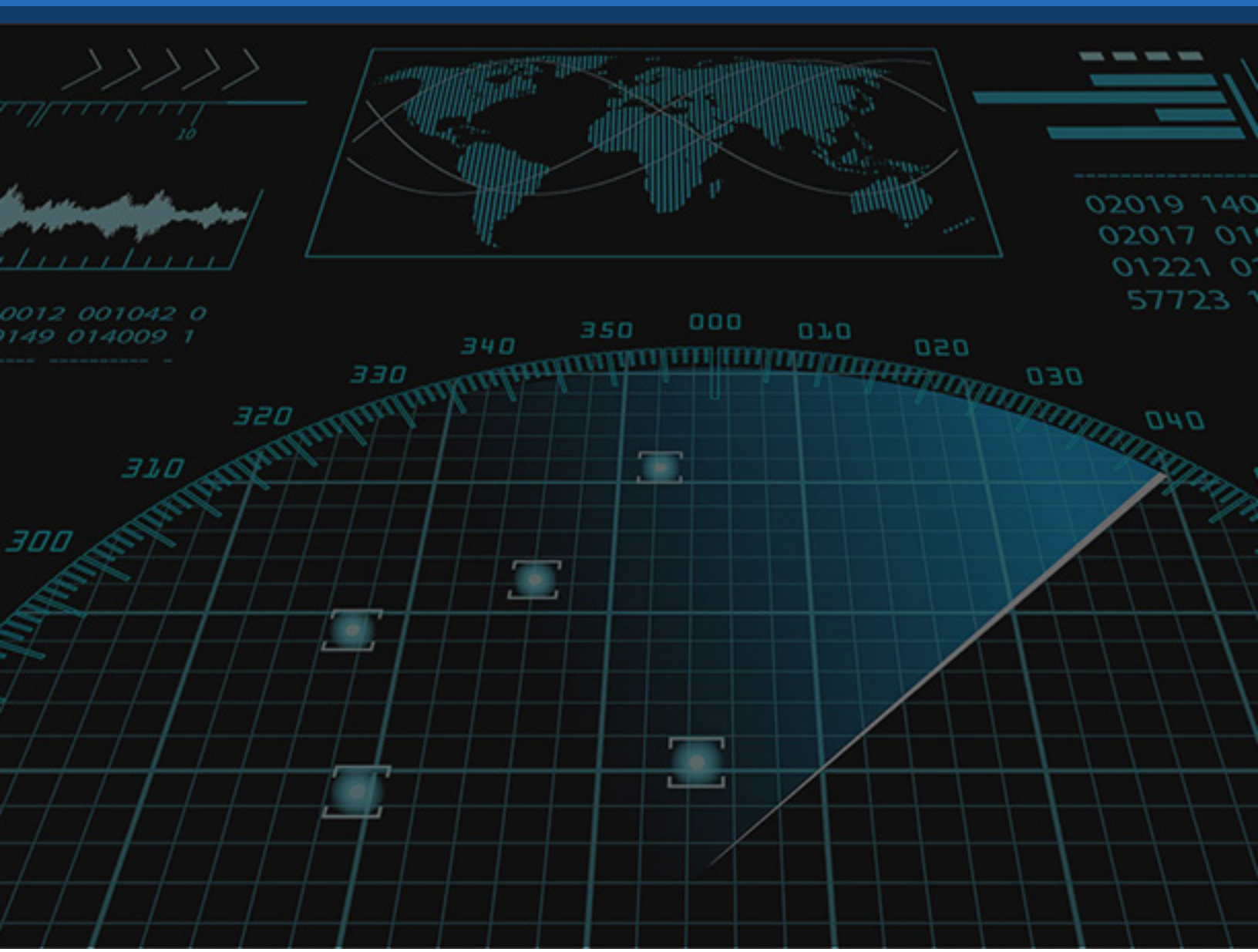
SPECIAL REPORT

Cyberwar and the future of cybersecurity



TechRepublic

ZDNet

Special report: Cyberwar and the future of cybersecurity

Published by TechRepublic
September 2016

Disclaimer

The information contained herein has been obtained from sources believed to be reliable. CBS Interactive Inc. disclaims all warranties as to the accuracy, completeness, or adequacy of such information. CBS Interactive Inc. shall have no liability for errors, omissions, or inadequacies in the information contained herein or for the interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

TechRepublic
9920 Corporate Campus Dr.
Suite 1000
Louisville, KY 40223
Online Customer Support:
http://techrepublic.custhelp.com/

Credits

Editor In Chief
Jason Hiner

Managing Editor
Bill Detwiler

Feature Editors
Jody Gilbert
Mary Weilage

Graphic Designer
Kimberly Smith

Contents

Cybercrime and cyberwar: A spotter's guide to the groups that are out to get you

By Charles McLellan

Cybercriminals are as varied as other internet users: just as the web has allowed businesses to sell and communicate globally, so it has given fraudsters the ability to plunder victims anywhere and set up crime networks that, previously, would have been impossible.

The web has become central to the smooth running of most developed economies, and the types of cybercrime have changed too. While 15 years ago the majority of digital crime was effectively a form of online vandalism, most of today's internet crime is about getting rich. "Now the focus is almost entirely focused on a some kind of pay-off," says David Emm, principal security researcher at Kaspersky Lab.

That's causing significant costs to businesses and consumers. IBM and Ponemon Institute's 2016 Cost of Data Breach Study found that the average cost of a data breach for the 383 companies participating increased from $3.79m to $4m over 2015: the average cost paid for each lost or stolen record containing sensitive and confidential information increased from $154 in 2015 to $158. All the organisations in the survey had experienced a data breach ranging from 3,000 to 101,500 compromised records, and the majority of the leaks were down to malicious attacks (as with many types of crime, the costs of cleaning up can be vastly higher than the loot that the hackers manage to get away with).

Data breaches aren't the only costs to business of online criminals: the FBI calculates that CEO email scams—where criminals pose as senior execs and persuade finance managers to transfer huge sums to phoney bank accounts—have hit tens of thousands of companies and cost over $3.1bn since January 2015.

There's a significant cost to business of protecting against attacks, too: according to analyst firm Gartner, worldwide spending on security products and services will reach $81.6bn (£62.8bn) this year, up eight percent year-on-year thanks to increasingly sophisticated threats and a shortage of cybersecurity professionals.

Most internet crime is motivated by a desire for profit—stealing banking credentials or intellectual property, or via extortion for example. But as online crime has grown it has also evolved—or mutated—into a set of occasionally overlapping groups that pose distinct threats to organisations of different sizes.

These groups have different tools, objectives and specialities, and understanding this can help defend against them.

Disorganised crime

"The bulk of cybercrime is the equivalent of real-world opportunist thieves," says Emm. These are the crooks you're most likely to come across, or at least feel the impact of, as an individual—the petty criminals of the

online world. They may spew out spam or offer access to a botnet for others to run denial-of-services attacks, or attempt to fool you into an advance-fee scams where the unwary are promised a big payday in return for paying (often a substantial) sum of money up-front.

One big growth area here is ransomware: "The return on investment in the criminal ecosystem is much better if you can get your victims to pay for their own data," said Jens Monrad, global threat intelligence liaison for FireEye.

Still, basic IT security is often enough to keep this sort of crime at bay: encrypting data, using anti-malware technologies and keeping patching up to date means "you're going to be in fairly good shape," according to Kaspersky's Emm.

Organised crime

"The twenty-first century digital criminal is best characterised as a ruthlessly efficient entrepreneur or CEO, operating in a highly developed and rapidly evolving dark market... they are a CEO without the constraints of regulation or morals," warned a recent report from KPMG and BT titled Taking the Offensive.

These groups will have a loose organisation and may utilise many contractors—some expert at developing hacking tools and vulnerabilities, others who will carry out the attack and yet others who will launder the cash. At the centre of the web is a cybercrime boss with the ideas, the targets and the contacts.

These are the groups with the capability to mount attacks on banks, law firms and other big businesses. They might execute CEO frauds, or simply steal vital files and offer to sell them back again (or sell them on to unscrupulous business rivals).

According to European law enforcement agency Europol in its 2015 Internet Organised Crime Threat Assessment, there is now some overlap between the tools and techniques of organised crime and state-sponsored hackers, with "both factions using social engineering and both custom malware and publicly available crimeware". Organised cybercrime groups are also increasingly performing long-term, targeted attacks instead of indiscriminate scatter-gun campaigns, said the agency.

When nation states use a technique it usually takes around 18 to 24 months for that to filter down to serious and organised crime.

"One of the challenges for the ordinary company is the level of the adversary continues to get more sophisticated because they are able to get access to more of the technologies than they would have been able to do in the past", said George Quigley, a partner in KPMG's cyber security division.

And it's not just the big companies that may be at risk. "You could be forgiven as a small business for thinking 'I'm not one of those guys, why would somebody want my network?'—but you are part of somebody's supply chain," said Kaspersky's Emm.

Hacktivists

These may be individuals or groups driven by a particular agenda—perhaps a particular issue or a broader campaign. Unlike most cybercriminals, hacktivists aren't out to make money from their exploits, rather to embarrass an organisation or individual and generate publicity. This means their targets may be different: rather than a company's accounts system or customer database, they may well want to access embarrassing emails from the CEO or other company officials.

"Networks that control much of our critical infrastructure—including our financial systems and power grids—are probed for vulnerabilities by foreign governments and criminals."
—President Obama

Terrorists

Despite the hype, the threat from cyber terrorism remains low, largely because these groups lack the skills, money and infrastructure to develop and deploy effective cyber weapons, which only the largest nations can hope to build. "Terrorist sympathizers will probably conduct low-level cyber attacks on behalf of terrorist groups and attract attention of the media, which might exaggerate the capabilities and threat posed by these actors," said US director of national intelligence James Clapper in his assessment of worldwide cyber threats in September last year.

State-backed hackers

While standard criminality accounts for the vast majority of cyber threats, the use of the web by state-sponsored hackers has been widely publicised in recent years. Much of this takes the form of cyber espionage—attempts to steal data on government personnel or on expensive defence projects. Governments will spend millions on developing all-but-undetectable ways of sneaking onto the systems of other nations—or those of defence contractors or critical national infrastructure—and these projects may take years of development.

"Networks that control much of our critical infrastructure—including our financial systems and power grids—are probed for vulnerabilities by foreign governments and criminals," warned President Obama last year, blaming Iranian hackers for targeted American banks and North Korea for the attack on Sony Pictures that destroyed data and disabled thousands of computers.

Like hacktivists, state-sponsored groups aren't usually seeking financial gain. Rather, they are looking to support the policies of their government in some way—by embarrassing another government by revealing secrets, or by gaining a potential strategic advantage, for example.

Worse, nation-state hackers may be interested in creating physical effects by digital means—bringing down a power grid or forcing open the doors of a dam at the wrong time, for example. This is where cybercrime tips over into cyberwarfare.

"The management and operation of critical infrastructure systems will continue to depend on cyber information systems and electronic data. Reliance on the power grid and telecommunications will also continue to increase, as will the number of attack vectors and the attack surface due to the complexity of these systems and higher levels of connectivity due to smart networks. The security of these systems and data is vital to public confidence and safety," says Europol.

With the emergence of the Internet of Things (IoT)—where everyday objects from thermostats to home security systems—can be controlled online, the risk of well-funded groups attempting to hack into these devices increases. If your organisation is being attacked by state-sponsored groups, keeping them out is likely to be extremely difficult: you should consider how to limit the damage, by segmenting networks and encrypting sensitive data, for example. Concentrating on blocking at the perimeter will not be enough.

Insider threats

With all the focus on external threats, is it possible that companies are forgetting a danger much closer to home?

"There's been an awful lot more issues being driven from insiders of late. One of the challenges is that when people think cyber they automatically think external," says KPMG's Quigley. Confidential company documents stored on shared drives and weak internal controls on who can access data mean that the disgruntled or greedy insider could still be one of the biggest risks to businesses. "They should have insiders much higher on the radar than they do," Quigley warns.

Blurred lines

In reality there's a lot of overlap between these groups, in personnel, the tools they use and the targets they choose. "The cyber threat landscape is becoming a much more complicated environment to do attribution or explain attacks," says FireEye's Monrad.

However, most breaches start in the same way, says Kaspersky's Emm: "What they have in common is how they get their initial foothold through tricking individuals into doing something that jeopardises security: click on a link, open an attachment, give out some confidential information." It's vital to educate staff and close obvious holes: through to 2020, 99 percent of vulnerabilities exploited will continue to be ones known by security and IT professionals for at least one year, according to Gartner.

What's certain is that, as the internet becomes even more essential to our day-to-day lives, the potential for cyber criminals to make money will only increase.

Devastating attacks to public infrastructure "a matter of when" in the US

By Teena Maddox

Cyberattacks have already impacted public infrastructure in other countries and it's only a matter of time until a similar attack results in a major catastrophe disrupting crucial services in the United States, according to IoT security experts.

"I think that it's definitely not a matter of if, it's a matter of when," said Zulfikar Ramzan, CTO of RSA and former chief scientist of Sourcefire. Ramzan is also the co-author of *Crimeware: Understanding New Attacks and Defenses*.

Public infrastructure refers to whatever is critical to keep society functioning, from utilities and water to hospitals, transportation and public safety. This infrastructure can be part of either the public or private sector, such as with financial services, hospitals and pharmaceutical companies. If any part of this structure is attacked, it could lead to an unprecedented crisis.

Overall, industrial control systems (ICS) incidents, as these type of attacks are known, are on the rise. The number of incidents reported to U.S. authorities increased 17 percent in 2015, with 295 incidents, according to the U.S. Department of Homeland Security ICS Cyber Emergency Response Team (ICS-CERT).

"This is a near-term threat that we need awareness about. We need to be prepared. From a general industry perspective, we see these industries taking a very compliance-driven approach. I draw direct parallels to what we've seen in enterprise security. Ten years ago everyone was taking a checklist compliance certification and accreditation and that gave them a false sense of security," said Brad Medairy, senior vice president at Booz Allen Hamilton and a leader of the firm's Strategic Innovation Group (SIG) and Predictive Intelligence business. "I see that today on the operational technology side, which is compliance driven and it's just a matter of time before sophisticated adversaries with malicious intent start to compromise that."

Ports, dams, railways, pharmaceutical manufacturers and utilities are at a high risk, along with supply chain problems within the manufacturing sector. "I think manufacturing in the near term is certainly at risk. I think that we're going to start to see potential ransomware, supply chain attacks and disruptions," Medairy said.

Tim Herbert, senior vice president of research and market intelligence for CompTIA, said, "I think today anything that is connected is a target. We have seen the trend over time that with many of the motivations for targeting, whether it's a business or infrastructure, is that there's much more of a monetary motivation, whether there's an expectation to extract funds via ransomware or a way to steal data to be able to monetize that in some way."

Ransoming the power grid is an inevitable attack, Herbert said, adding, "governments are really struggling to try to reconcile some of these challenges and what to do, such as not jumping to conclusions—especially when it's so easy to create an attack and make it seem like it's coming from another country. We know an attack is coming, it's just a matter of what the degree and the intensity of it is."

A nuclear power plant in Germany was infected with malware as the result of employees bringing in USB flash drives from the outside. And malware was found in the control room of a Japanese nuclear reactor.

Other countries have already suffered at the hands of cunning cybercriminals hacking into the public infrastructure:

- In December last year, more than 225,000 customers in the Ukraine experienced a blackout on a cold winter's day as the result of remote intrusions at three regional electric power distribution companies. Hackers thought to be associated with Russia were blamed for the attack that used malware to attack and destroy data on hard drives and flood phone lines with a denial-of-service attack, according to a U.S. Homeland Security report.
- North Korea has been tied to three separate reconnaissance attacks on South Korea's light rail operators, stealing information pertaining to critical systems such as speed and safety controls, according to a report by Booz Allen Hamilton.
- A nuclear power plant in Germany was infected with malware as the result of employees bringing in USB flash drives from the outside. And malware was found in the control room of a Japanese nuclear reactor.

People in the U.S. have more of a tendency to wait until something happens here to be concerned about the risk, according to Scott Montgomery, CTO of Intel Security for the public sector.

"Our way here is to wait until our nose is rubbed in it before we do a lot to be proactive. Imagine if the 200,000 had been in Pittsburgh, Pennsylvania rather than the Ukraine. You might not have even covered the Ukraine incident. But imagine if it happened in Pittsburgh—we'd still be talking about it," Montgomery said.

"There are some organizations doing a little bit more because they don't want to be on the front page. The United States Army asked Congress for an additional $200-some million dollars so they could gain power grid independence and become an independent power generator, so they didn't have to rely on the grid at Fort Bragg and Fort Hood respectively. They said if someone turned out the lights in Killeen, Texas it would seriously impact our war fighting ability. We need independence from that," said Montgomery. Fort Hood is located in Killeen, Texas.

Another city that's taking preventative measures is New York, N.Y., which tests water from an aquifer 80 miles away to make sure that nothing has been added to the water supply. By testing so far from the city, they can isolate problems before the water supply reaches the metro area, Montgomery said. "But every municipality doesn't have the wherewithal or the ability to do that," he added.

Despite the belief that critical infrastructure networks can be 'isolated' or 'air gapped,' and cannot be attacked from the outside, hackers always find a touch point between the sensitive operational network and the open IT network, said Daniel Cohen Sason, software engineer manager for Cyberbit. This then "exposes the critical ICS/SCADA networks to external attacks. Since OT networks are based on legacy devices and non-standard protocols, network managers are often unaware of these touch points, which makes the threat of a hack even more likely than it was previously thought to be."

"A lot of the IoT we've been looking at are consumer devices and they're woefully lacking in security because security is hard to set up. It's been an almost deliberate decision by manufacturers to make them easy to hack into."
—Timo Elliott

"The effect on public infrastructure could be a power outage, like we saw last year in Ukraine. Or, it could be something more serious like a Chernobyl-style catastrophe at a nuclear plant. The problem we often see is that critical infrastructure network operators are notoriously reluctant to introduce security products into their fragile, legacy networks, which leaves the door open to hackers with malicious intent," Sason said.

There's particular concern among the water supply and dams because there isn't a strong focus on security. "We see some crazy things when we go out and look at client environment in those industries," said Medairy, particularly with employees using traditional IoT devices for their personal use and connecting them to the internet while they're at work.

IoT products as a whole aren't built with enough security in place, according to Matt Scholl, computer security division chief for the National Institute of Standards and Technology (NIST), which produced a report in July on the topic and recommends a framework for improving critical infrastructure cybersecurity.

"It really would be nice if IoT products were built with a least functionality and a security capability as part of them. That would be awesome. And it would be great if us as a market...emphasized and incentivized that to IoT vendors. They will build it, but we have to come," Scholl said. "We need to somehow incentive and reward people who are doing security and reliability and privacy engineering into these products so that they will do it. Rather than waiting for the crisis to happen."

Timo Elliott, vice president and global innovation evangelist for SAP, said, "A lot of the IoT we've been looking at are consumer devices and they're woefully lacking in security because security is hard to set up. It's been an almost deliberate decision by manufacturers to make them easy to hack into."

"Every network is always under attack," Elliott said. "It's important to design these systems to prevent attacks. There will always be tiny cracks you can't find or block, like with bugs in your house. You need an onion approach with more layers."

The key to surviving such an attack is to recognize the reality that it will be impossible to keep every hacker from getting into the front door of an organization's network, Ramzan said.

"We can still prevent them from getting much past the front door, if they get in. The goal of an attacker isn't to compromise an IoT device or a server somewhere for its own sake—they're after something deeper and more insidious for the attacker. There is time from the entry to the overall breach," Ramzan said, explaining that a company needs to figure out how to minimize that window and quickly detect the hacker to stop them from achieving their main goal, whatever that might be.

Companies spend a disproportionate amount on prevention, and that leaves nothing for dealing with detection and response after there's a breach. With Gartner predicting 6.4 billion connected devices by the end of this year, and upward of 21 billion connected devices by 2020, the risk of a hacker attacking public infrastructure will only get worse with time, Ramzan said.

"The real key in being able to solve that problem is going beyond visibility and coupling that with analytics," he said. "Analytics is about being able to glean meaningful nuggets of insight from that sea of noise. If you can do that intelligently then you can really provide an organization with prioritized lists of what they need to do to reduce their risks as quickly as possible. I call that 'the gap of grief.' Security is no longer an IT concern. It's a CEO board-level concern."

Understanding the military buildup of offensive cyberweapons

By Conner Forrest

"Shall we play a game?"

"Love to. How about Global Thermonuclear War?"

True geeks will recognize the above exchange as one of the seminal pieces of dialogue from the 1983 film *WarGames*, where a young hacker named David Lightman nearly starts World War III after gaining access to a powerful military supercomputer. The film was a critical success and set the stage for a variety of films that explored the relationship between cybersecurity and the military.

The rise of offensive cyberweapons has changed the landscape of cyberwar from protecting against data theft to defending against physical destruction.

WarGames, and films like it, were meant to be perceived as fictional. As time has gone on, though, the line between what kinds of cyberwarfare are possible and what is science fiction has begun to blur. Computer programs like the Stuxnet worm, for example, have taken down large portions of government infrastructure, such as some of Iran's nuclear centrifuges.

But when and how did this happen? The rise of offensive cyberweapons has changed the landscape of cyberwar from protecting against data theft to defending against physical destruction. To understand this rise, it's helpful to look at the history of such weapons.

The birth of offensive cyber

There's much confusion around some of the language used when referring to elements of cyberwarfare. Ewan Lawson, senior research fellow of military influence at RUSI, said that it is important to clarify that offensive cyberweapons don't typically deal with passive activities like data collection or surveillance. Rather, a cyber-weapon is something that is "deliberately designed to do damage or destruction."

Bob Gourley, co-founder of the cyber security consultancy Cognitio and former CTO of the Defense Intelligence Agency, echoed that sentiment. According to Gourley, at least in the US, "offensive cyber weapons are not designed to take information, but to degrade, disrupt or destroy systems."

Cyberwarfare, and the offensive weapons associated with it, have been around for a long time. Gourley, and others, would argue that these weapons have been around since the US Civil War, when both sides began destroying the telegraph lines that carried vital information. As technology progressed, military targets continued to be attacked, but civilian infrastructure did as well, Gourley said.

"I would suspect that, since the beginning of networking, there's been cyberwars going on, but we just haven't known about them," said Forrester analyst John Kindervag.

More recently, though, major cyberattacks have come to light that showcase just how powerful cyberweapons can be. Perhaps the most notable of these is Stuxnet, a computer worm that caused some Iranian nuclear centrifuges to self-destruct.

"Stuxnet is interesting in that it was one of the first incidents where cyber accesses, effectively, were used for destructive purposes," Lawson said. "Prior to that, there might have been some deletion of data, there have been DDoS-type attacks, but Stuxnet is one of the firsts where you see actual, physical destruction as a consequence of an attack through cyberspace."

Of course, that's just the surface-level effect. Stuxnet also proved how far some entities are willing to go to successfully carry out an offensive cyberattack. Kindervag said that tools like Stuxnet were obviously not built overnight, and some experts on the development of such tools have estimated that if it were built as a commercial product, the development costs would be around $100 million.

The Stuxnet worm was uncovered by accident, when its source code escaped into the wild. Scott Warren, a partner at Squire Patton Boggs, which specializes in cybersecurity, said that this presents another serious problem.

"The worry here is that it has mapped a blueprint for the next generation of cyberwarfare: From the previous being focused on corporations and individuals—and which were primarily financially motivated—to one where an attack on a city's infrastructure is now possible," Warren said.

Still, Stuxnet isn't the only attack of its kind to make headlines. Around the same time that the famous Sony hacks were coming to light, a cyberattack was used to cause massive destruction at a German steel mill, Lawson said. And even more recently, hackers were able to attack Ukraine's power grid and shut off power in some areas.

Despite these things seeming to happen more often, it doesn't necessarily mean that the world is seeing a rise in the availability of cyberweapons. Lawson said that it's a matter of more opportunities presenting themselves, while Kindervag said that it could just be a matter of increased awareness.

On the flip side, Warren argues that there is evidence of a rise in the use of cyberweapons, but that it's important to understand the semantics around some of the phrasing.

"Under the UN definition, there have been very few attacks that would qualify as 'cyberwarfare,'" he said. "Perhaps many of the other examples are more 'cyber-terror,' where individuals act in a coordinated fashion—such as 'hacktivisits'—to disrupt or destroy infrastructure."

No matter the trajectory of modern offensive cyberweapons, the fact of the matter is that they're here and are bound to become more prevalent and more powerful as time goes on.

The reality of cyberwarfare

One of the other big questions to answer is this: Who has these weapons? Long story short—no one is entirely sure. When it comes to traditional weapons, like nuclear missiles, there are measures in place to track their origin of launch or to measure how much enriched uranium a country has stockpiled. For cyberweapons, it's far more difficult to track.

So far, we know that the US and UK have declared programs, Lawson said. China, Russia, Israel, and North Korea are all typically regarded as potential major players in cyberwarfare as well. But it's also plausible that many more groups are involved.

"My instinct and experience tells me that every nation state is involved in this," Kindervag said.

> "If a country goes rogue with chemical weapons, there will be sanctions placed on it by the UN or others. This is not yet the case for cyberwarfare."
> —Scott Warren

Even though it is unclear what capabilities many countries have, their responses to the rise of cyberwar have been more public. The US is especially open about this, declaring that it has two cyberspace weapon systems available and elevating its Cyber Command to a Unified Combatant Command (UCC). The US government has even declared cyber as the fifth domain of warfare—land, sea, air, space, and cyber.

Around the world, though, jobs have been popping up for government roles in cyber. Lawson said that the UK model tends to be mostly government-based, while the US model is a mix of contractors and government. The Russian model, he said, appears to be a combination of formal military service organizations and a willingness to use non-state groups and activists. China, on the other hand, is very military-focused. What's interesting to note, Lawson said, is that the patterns of approach to cyber among these countries are very mixed.

Despite these approaches, Warren said, there's still no governing body that deals with issues related to cyber-warfare.

"If a country goes rogue with chemical weapons, there will be sanctions placed on it by the UN or others," Warren said. "This is not yet the case for cyberwarfare. Proving who was behind a given attack is also difficult, with some countries pointing the finger at a group of patriotic hackers. No government has admitted any role in Stuxnet, for example."

These risks affect business and consumers as well. For instance, if a business is working with the government, or providing a product for them, it will be targeted. One example is Lockheed Martin, which had its plans for the F-35 stolen, Lawson said.

A challenge for both businesses and consumers is the potential for attacks on infrastructure. Attacks such as one that would shut down a power grid would be early aims in a cyberwar, Lawson said. And while the effects are often temporary, a cyberattack on a power grid could cost billions of dollars.

Critical national infrastructure like water and power come into play, but nontraditional infrastructure will also be targeted.

“What about things like food distribution networks in the West, where everything is ‘just enough just in time?’ It wouldn’t take much to disrupt those to the point where there’s no food on the shelves,” Lawson said.

Despite the increased risk brought about by cyberwarfare, some experts argue that there is an intrinsic value that comes with its rise. Both Gourley and Kindervag said that the use of Stuxnet possibly saved the involved parties from a ground war. One could hypothesize, Kindervag said, that Israel might have felt it necessary to attack the nuclear refineries in Iran if they hadn’t first been disabled by Stuxnet.

An additional argument could be made that if war has to happen, it would be better if it was perpetrated in cyberspace instead of the real world.

“If we’re going to have warfare, the cyber world is a pretty bloodless place to do it,” Kindervag said.

Cybercrime Inc: How hacking gangs are modeling themselves on big business

By Danny Palmer

The clichéd image of a cybercriminal is one of a lone hacker, huddled over a computer in their parent's basement. Today, that stereotype couldn't be further from the truth, because—now more than ever—cybercrime is carried out by gangs running sophisticated operations.

"Advanced cybercrime groups now mirror legitimate organizations in the way they operate, with networks of partners, associates, resellers, and vendors.
—Sian John

The most organized criminal groups, such as those active on the dark web, are operating like legitimate businesses, with departmentalized teamwork, collaboration tools, training, and even service agreements between malicious software providers and their hacker customers.

"When you start to see malware kits that have customer service agreements and warranties associated with them, you know that you've moved into a pretty professional space," says Nathaniel J Gleicher, former director for cybersecurity policy for the White House's National Security Council.

Like the legitimate software market, cybercrime is now a huge economy in its own right, with people with a range of skillsets working together towards one goal: making money with illicit hacking schemes, malware, ransomware, and more. It's essentially an extension of 'real world' crime into cyberspace, and it's come a long way in recent years as groups have become bigger, more specialized, and more professional.

"There's been a substantial amount of improvement and innovation in the way attackers go after networks and, as cybercrime has professionalized, you've seen individuals develop a particular set of skills which fit into a broader network," says Gleicher, now head of cybersecurity strategy at Illumio.

"You have people who are managing and distributing credit card information, people who are cracking bank accounts, people who are managing remote access toolkits, to people who specialize in social engineering. There're very specific skillsets," he adds.

But it's not just gangs of hackers anymore: the cybercriminal ecosystem has evolved to the extent that it supports roles you'd expect to find in any large business.

"Advanced cybercrime groups now mirror legitimate organizations in the way they operate, with networks of partners, associates, resellers, and vendors. Some groups even deploy call center operations to ensure maximum impact for their scamming efforts," says Sian John, chief strategist for EMEA at Symantec.

That overlap with the world of business is also true of the tools cybercriminals use to communicate and collaborate, with different groups—whether they're responsible for orchestrating phishing campaigns or stealing and cloning card data—coordinating their actions for maximum effect.

"They're very much acting like a business. We're seeing that they very much collaborate and communicate via encrypted instant messaging systems," says Jens Monrad, senior intelligence analyst at FireEye.

However, such systems aren't open to anyone, as the dark web is still very much a closed space. "They're still using various internet forums, some which are only available if you have enough street credibility or that you have to pay for to demonstrate how you're willing to collaborate on their terms," Monrad says.

Terms and conditions have very much become a part of the increasingly professionalized world of cybercrime, where cybercriminals are now leasing out or franchising their malicious software as a service and making just as much money—if not more—than when they were selling it themselves.

"The franchises take that technology, but rather than hosting it in the country where it's being developed, they'll ask the developers if they can take some of their services and host them in places they can't get to and let them take a cut. It's exactly the same as an independent software company: they have their own channel programme," says Bharat Mistry, cybersecurity consultant at Trend Micro, who describes such operations as "full-on enterprises on the underground".

This practice of hosting services to allow foreign cyberattackers to more easily commit cyberattacks against local targets has been observed in China and Russia. It's systemic of what has become a global trade meaning, like the largest enterprises, cybercriminal outfits are able to operate around the clock.

With 24-hour operations in what looks increasingly like a service-based business, cybercriminals are even recruiting people to work as customer service operatives—although many of these 'employees' will be unaware they're working for a criminal group.

"Some groups deploy call center operations to ensure maximum impact on their scamming efforts and, in some instances, employees of the call center are oblivious to the fact they are working for criminal groups executing low-level campaigns like tech support scams," says Symantec's Sian John.

If traced by the authorities, the people unwittingly aiding these criminal activities might be fined or worse. But while these individuals might be discovered, the gangs they are working for often remain in the shadows.

Cybercrime credentials

While those at the bottom are unskilled, the professionalization of cybercrime has brought about another initiative you'd expect to see in any legitimate business operation: training courses. These programs are offered on the dark web in exchange for Bitcoin, the preferred currency of organized cybercriminal groups.

"There are online training courses you can pay for which show you how to go about hacking a website and infiltration. Everything which happens in physical enterprises is happening in the cybercriminal underground," says Trend Micro's Mistry, adding "it's only a matter of time" before this becomes a widespread activity within the professional cybercriminal economy.

"We should assume any training techniques which are being used in legitimate organizations are being used in cybercriminal organizations as well," agrees Illumio's Gleicher.

Gleicher investigated and prosecuted cybercriminals during his time at the US Department of Justice and therefore has first-hand experience of just how sophisticated these schemes have become.

"What I found most interesting in the rise of professionalization is, as you're tracking these institutions, you quickly find they're based in multiple countries and they have sophisticated coordination frameworks to work together," he says.

What he took away from the experience was that cybercriminal operations are becoming increasingly niche, with groups conducting every type of cyberfraud using strategic business techniques that rival those used within corporations.

"They're working together in this really clockwork way, they'll specialize. So if you see an organization which runs fraud scams, something as simple as selling fake cars online, they're going to specialize in that and they're going to have teams of people creating legitimate looking websites, and teams of people communicating with prospective buyers who have effective enough English to appear legitimate," Gleicher says.

These trends suggest that hacking and cybercrime are no longer the domain of individuals seeking to make a nuisance of themselves. Cybercrime is now an industry involving major criminal groups, with ecosystems as well-structured as the corporations they're likely attempting to target. Organizations must therefore ensure their own defenses are up to fighting this threat.

Why ransomware is exploding, and how your company can protect itself

By Alison DeNisco

Ransomware represents a growing threat for the enterprise, as 40 percent of businesses worldwide were attacked with their data held ransom in the past year.

This particular brand of malware is not new: The first recorded case of ransomware, known as the AIDS trojan, appeared in 1989. The attack is relatively easy to deploy and cash in on, said Michael Canavan, vice president of presales systems engineering at Kaspersky Lab.

In the past, cybercriminals targeted a wide range of consumers, and would ask for around $300 to release their personal photos and information. Between April 2015 and March 2016, more than 718,500 users were hit with encryption ransomware—an increase of 550 percent compared to the same period in 2014-2015, according to Kaspersky Lab research.

"The way it's going, we don't see any indication that the growth rate is slowing," Canavan said.

Once businesses started getting infected, hackers realized payoffs could get higher, Canavan said. "Business targets are at a higher premium because they have a bigger resource pool and more capabilities in terms of data—it's not just photos of your kids, it's patient files in hospitals and financial records in banking organizations," Canavan said. "Asking for a couple hundred bucks might not justify the value of the data encrypted."

Ransom costs are rising along with the attacks: The average ransom amount for 2015 was about $680—nearly twice that for 2014, according to a Symantec report. It will likely double again in 2016, said Kevin Haley, Symantec's director of security response.

The majority of ransomware attacks are not targeted toward one particular end user or business—rather, they cast a wide net via a phishing email, and then infect a user's home or work device, Haley said. Still, about 43 percent of spear phishing attacks (malware hidden in messages that appear to be from a trustworthy source) include ransomware targeted at small businesses in 2015, up from 34 percent in 2014, another Symantec report found.

Hospitals are also becoming lucrative prey, in part due to high-profile attacks where healthcare organizations paid thousands to hackers. They also tend to have lots of sensitive material on file and outdated security practices, said Gartner analyst Peter Firstbrook.

Broken down by industry, some 38 percent of attacks are in the services field, which includes health care. About 17 percent of attacks are in manufacturing, just over 10 percent are in public administration, and nearly 10 percent are in finance, insurance, and real estate, according to Symantec. The US is the most affected region, with 28 percent of global infections, the report found.

One of the most popular vehicles for ransomware is a phishing email telling the user they have an invoice that requires payment, Haley said. Another common way is to infect a website, or redirect one website to another hosting the malware.

Haley expects to see more targeted attacks against businesses over the next year, and for other devices to come into play. Strikes on computers and smartphones are the norm, but they could also occur on any IoT device, from smart TVs to refrigerators to watches.

"Ransomware is real, and it's going to affect your organization," Haley said. "Most of the steps to protect yourself are not unique—in the end, protecting yourself against ransomware will protect you against other security issues as well."

Best practices for your company

IT leaders should continuously seek out innovative technologies to add to their customized, layered defense, said James Scott, senior fellow and co-founder of the Institute for Critical Infrastructure Technology. "Look at where your valuable data is, who is trying to exploit it, and what vulnerabilities are there in protecting it," he added.

To prevent a ransomware attack on your company, experts say IT leaders should do the following:

- Use a layered security approach, with all endpoints protected, as well as protection at the mail server and gateway. "If you can stop these things from ever showing up in an end user's mailbox, you're ahead of the game," Haley said.
- Educate your employees. "The human element is always going to be the weakest element," Scott said. "The organization's infosec team has to continuously update their education for other staff with relevant threats."
- Run risk analyses, and patch vulnerabilities, especially on browsers, browser plugins, and operating systems. "Infosec teams should be savvy enough to continuously pen test the organization to hunt for vulnerabilities," Scott said. "It's important that they do that with the same vigor as the adversary would."
- Build a comprehensive backup solution, and backup often. "If your files get encrypted, you don't have to pay the ransom—you just restore the files," Haley said. Most businesses back up, but some have not tested whether or not these backups work in an emergency.
- Track behavior analytics to detect abnormalities among users.
- Limit access to file shares to only those who absolutely need access.

Some organizations are using AI products to predict threats, Scott added. "A year ago, the technology to detect and respond to threats was what everyone was talking about," he said. "Now, it's detect, respond, and predict."

How the Dark Web works

By Dan Patterson

The Dark Web is an ominous network of shadowy hackers hellbent on stealing company data, overthrowing the country, and selling drugs to your kids with Bitcoin.

Or is it? The hidden and encrypted internet enables hackers and activists and criminals. It's also a wonderful source for shocking headlines and salacious YouTube stories, and a communication and privacy-enhancing platform. Powered by a network of encrypted websites and accessible only by using a complex set of security tools, the Dark Web is as intriguing as it is beguiling. To understand the realities of the hidden internet, better grab a flashlight.

The Dark Web and the deep web are terms often confused and used interchangeably. The deep web is a term that refers to sites and pages unavailable to the general public and not indexed by traditional search engines, like corporate intranet sites, private social media posts, and pages with nofollow search tags.

Above the deep web hovers the clearnet, the traditional internet and mobile web used by billions of people around the world. The clearnet is secure, and encryption is used to move secure data from place to place all the time. SSL guards passwords and protects credit card information during e-commerce transactions. But the very nature of the clear internet is that anonymity is rare. Computer and mobile IP addresses are constantly logged and easily traced. Cookies help web marketers track online activity and analyze behavior.

What differentiates the so-called Dark Web is the method by which sites are accessed. The Dark Web, or darknet, is a network of sites with encrypted content, accessible only with a secure suite of secure-browsing tools, like Tor. Tor—an acronym for the onion router—is a package of open source security tools written for a customized version of the Mozilla Firefox browser, compatible with Windows, OS X, and Linux. The software encrypts user traffic and passes the IP address through the complex of Tor nodes.

These "onion layers" help protect the user's anonymity and allow users access to similarly protected websites. These sites range from forums to wiki pages to blogs and function much like clearnet sites. Dark Web domains frequently employ non-memorable, hashed URLS with the .onion top level domain. These sites block inbound traffic from all non-secure internet connections.

Personal and work computers often house mission-critical data, like sensitive files, passwords, and health records. Because Tor can be used and the Dark Web can be accessed on a traditional home PC, security professionals rely on additional security tools like the Tails operating system. Tails is a Linux distribution that can be installed on and run from a portable flash drive. By accessing the Dark Web Tails, user behavior is never logged locally, and it is significantly more challenging for malicious software to harm the host PC.

The Dark Web is used frequently by good actors for legitimate reasons. Encryption, security, and privacy are championed by news organizations, tech companies, universities, and activists in repressive regimes. The U.S.

State Department helps fund the Tor project, and according to the United Nations, encryption is a fundamental human right. Facebook operates a widely used secure Dark Web portal to the social network.

Yet it is also true that the Dark Web is an opaque, sometimes twisted, reflection of the clearnet. Crime is profligate. Black markets enable the morally libertine to profit handsomely in Bitcoin. The most famous Dark Web market, the Silk Road, allowed vendors and buyers to conduct business anonymously and enabled the sale of drugs, guns, humans, identities, credit card numbers, zero-day exploits, and malicious software. The site was raided and shut down by the FBI in 2013, but the idea of an anonymous, encrypted black market spread rapidly. Today, the site Deep Dot Web lists dozens of Dark Web markets.

Though it's not necessary for the layperson to visit the Dark Web often, if ever, every consumer is at risk of identity theft and should have a basic understanding of how the encrypted internet functions.

"The Dark Web operates a lot like the clear web," said Emily Wilson, Director of Analysis at security firm Terbium Labs. "The same crime that happens offline, all the time, also happens on the Dark Web." In many ways, she said, because it's relatively easy to visit Dark Web markets, it's sometimes easier to see criminal activity as it happens.

Though it's not necessary for the layperson to visit the Dark Web often, if ever, every consumer is at risk of identity theft and should have a basic understanding of how the encrypted internet functions. Businesses should be aware that data from hacked companies and the government is easy to find and purchase on the encrypted internet. A number of companies, including Tripwire, ID Agent, and Massive, monitor the Dark Web and help businesses respond to Dark Web data leaks.

The Dark Web is not entirely malicious, but it's also not a safe place to visit. Novices and experts alike should exercise care and caution when visiting the Dark Web. ZDNet does not condone illegal or unethical activity. Offensive material can sometimes be just a click away. Browse at your own risk. Never break the law. Use the Dark Web safely, and for legal purposes only.

The Dark Web—like encryption—is a double-edged sword. The hidden internet enables both good and bad actors to work uninhibited anonymously. And like encryption, the Dark Web is a reality for both consumers and business. Companies need to know about the Dark Web, Wilson said, and they need to be prepared for incidents to occur.

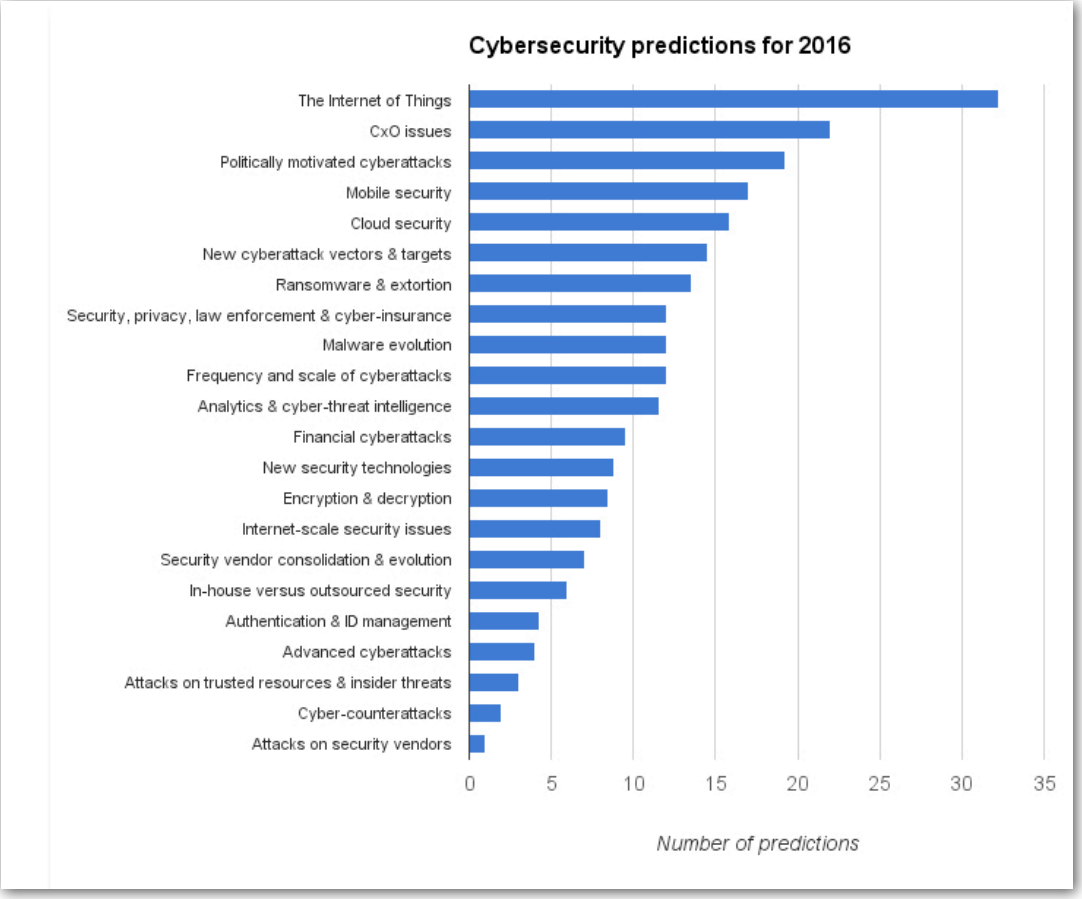
But consumers and companies shouldn't overreact to perceived threats. The Dark Web is not enormous. "Compared to the clearnet, the Dark Web is maybe a few thousand, or few hundred thousand [sites.]," Wilson explained. "Only a few thousand return useful content, and compared to the clearnet there's tiny amount of regular Tor users."

Cybersecurity predictions for 2016: How are they doing?

By Charles McLellan

Like death and taxes, few things are more certain than the annual deluge of cybersecurity breaches, which shows no sign of abating despite the best efforts of the 'good guys'—the security industry, CSIOs, government bodies, 'white hat' hackers, academics and others. Another fixture in the tech calendar is a spate of articles around the turn of every year that attempt to predict how the cybersecurity landscape will change over the next 12 months.

At the beginning of 2016, ZDNet's sister site Tech Pro Research examined 244 cybersecurity predictions for 2016 from 38 organisations, and assigned them among 22 emergent categories (occasionally splitting a prediction among two or three categories). The results were as follows:



Predictions from: A10 Networks, Appriver, AT&T, BAE Systems, Blue Coat, DataVisor, DomainTools, Experian, FireEye, Forrester, Fortinet, Hexis Cyber Solutions, HyTrust, IBM, Imperva, Kaspersky, Lancope, Lieberman Software Corporation, LogRhythm, McAfee, MWR Info Security, NSFOCUS Global, OpenSky/TUV Rheinland, Ovum, Palerra, PCI Security Standards Council, Proofpoint, Raytheon/Websense, RSA, Seculert, Sophos, Symantec, Technology Business Research, ThreatStream, Trend Micro, Varonis, Vectra Networks, ZScaler

Image:Tech Pro Research

Now that we're over halfway through the year, it's worth examining how the pundits' predictions are panning out: are we seeing an explosion in IoT-related incidents, for example—as the above graph suggests—or are some less-heralded cybersecurity issues dominating the headlines?

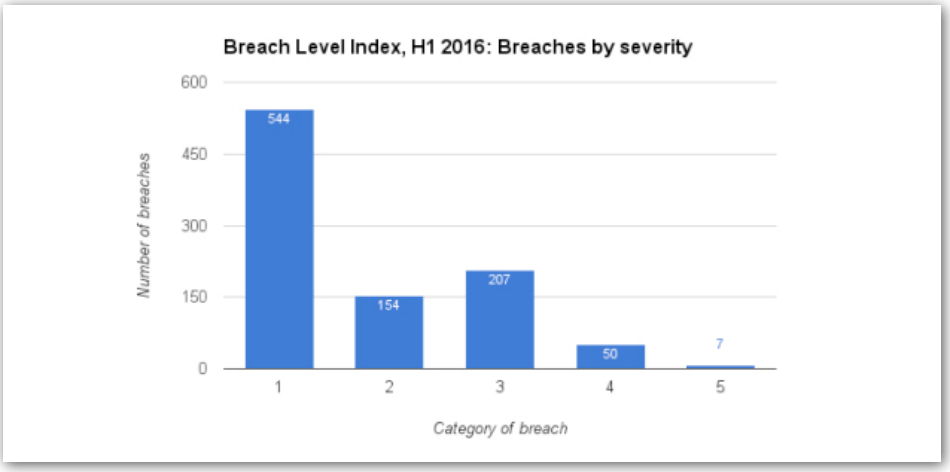
But first, let's look at some general trends.

Breach Level Index data

Security firm Gemalto's Breach Level Index (BLI) is a database that tracks publicly disclosed breaches across the globe, measuring their severity via a multidimensional index based on factors including the number of compromised records, the source of the breach and the type of breach. The index runs from 1-10 on a (base 10) logarithmic scale, as in the indices for volcanoes and earthquakes, so a score of 7 is ten times more severe than a score of 5.

These BLI scores can be mapped to a simple 5-point scale, ranging from Category 1 ("A breach with no material effect. Less than 1000 records. Notification required but little damage done.") to Category 5 ("A breach with immense long-term impact on breached organization, customers and/or partners. Very large amount of highly sensitive information lost [usually 10-100+ million records]. Massive notification process. Potentially existential financial loss for breached organization in remediation and related costs. Use of lost sensitive information seen.").

Here are the breaches for the first half of 2016 on this 5-point scale:

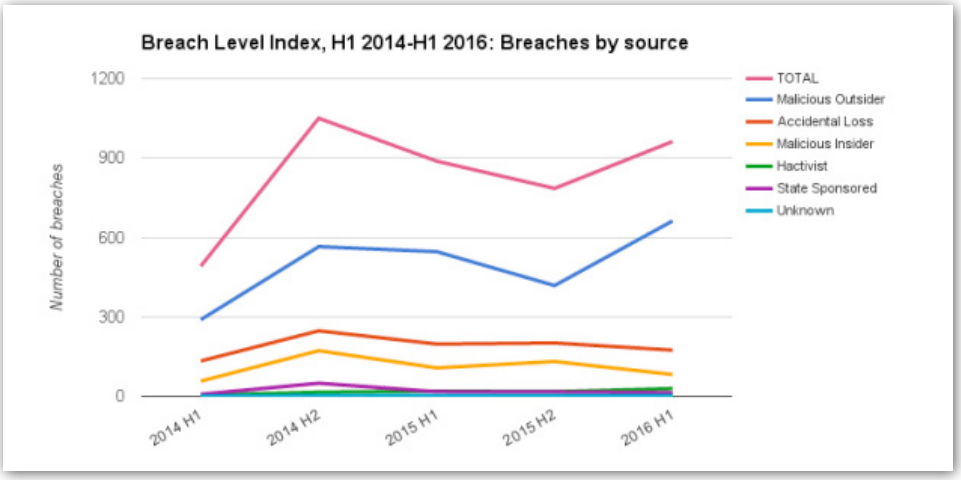


Data: Gemalto Breach Level Index/Image: ZDNet

The majority of H1 2016's publicly disclosed breaches—544 out of 962, or 56.5%—fall into the "Little damage done" Category 1, but there are 50 Category 4 breaches and seven Category 5 ones. The latter are headed by the 40 million records stolen from Fling.com, an adult dating website, and put up for sale on the 'dark web'.

The 962 breaches in H1 2016 resulted in 537 million compromised records, including 26 breaches with over a million records affected. However, the number of compromised records was unknown in 53 percent of the breaches. Comparable figures for the whole of 2015 are: 1,673 breaches; 707 million compromised records; 46 breaches with over a million affected records; and 47 percent of breaches with unknown numbers of compromised records. Clearly, there's no apparent let-up in the frequency and scale of cybercrime.

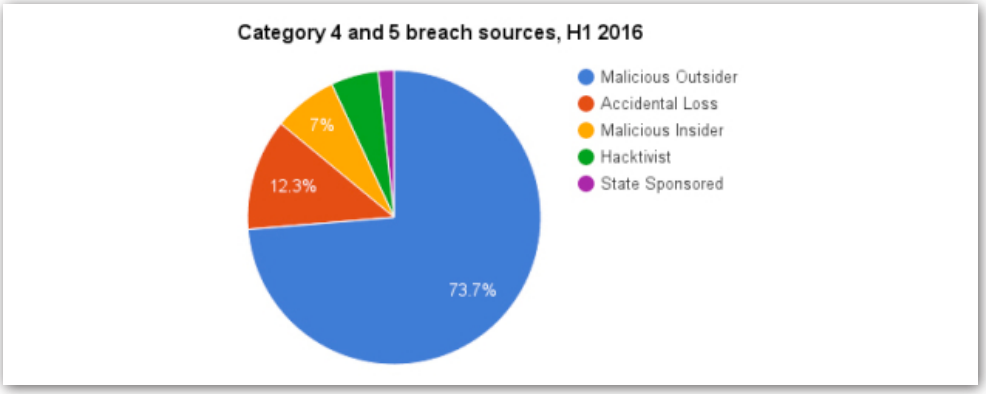
What are the sources of all these security breaches? Here's the BLI data going back to H1 2014:



Data: Gemalto Breach Level Index/Image: ZDNet

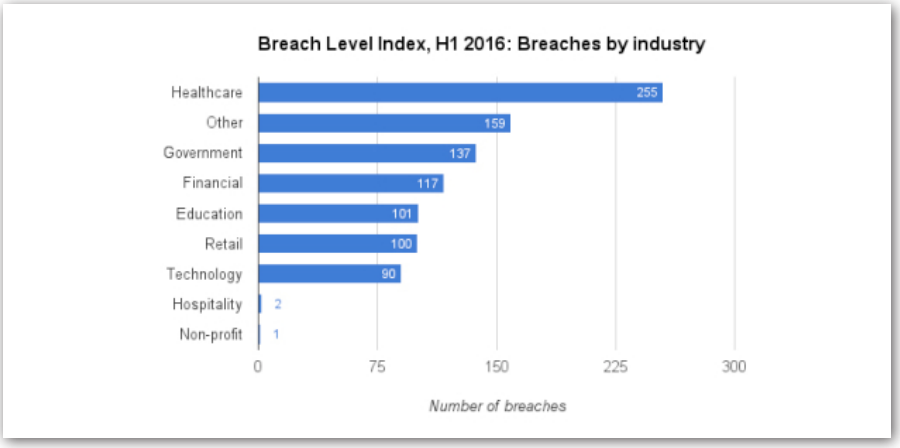
Malicious Outsiders are consistently the number-one source of breaches over the last two years, followed by Accidental Loss and Malicious Insiders. Hacktivist and State Sponsored breaches remain at low levels compared to this trio of 'traditional' sources.

This general pattern also holds when we look at just the biggest breaches (Category 4 and 5) reported in the first half of this year:



Data: Gemalto Breach Level Index/Image: ZDNet

As far as targeted industry sectors are concerned, healthcare leads the way in H1 2016 (as it has done for the past two years):



Data: Gemalto Breach Level Index/Image: ZDNet

By region, the overwhelming majority—757 out of 962 (79%)—of reported H1 2016 breaches occurred in North America. Bear in mind, though, that the stringency of reporting regulations vary around the world.

So far, then, 2016 appears to be 'business as usual' so far as large-scale cybersecurity patterns are concerned.

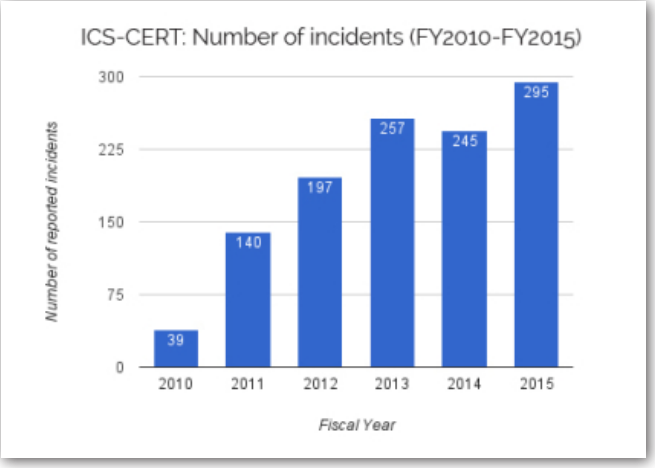
2016 predictions so far

Let's look at some the top prediction categories from the turn-of-the-year articles examined by Tech Pro Research (TPR) and see how the pundits have performed so far.

The Internet of Things

The fact that so many predictions for 2016 concerned the IoT—and critical infrastructure or the 'industrial' IoT in particular—is little surprise, given the prominence of the subject in recent years and the steady rise in IoT-related security incidents.

The US Department of Homeland Security's ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) documents industrial IoT incidents in the US, and has seen a more than seven-fold rise since 2010:



Data: ICS-CERT/Image: ZDNet

It will be interesting to see what the figures for FY2016 (Oct 2016-Sep 2016) look like, in due course. In FY2015, ICS-CERT found that Critical Manufacturing was the most attacked sector, ahead of Energy (the number-one target the previous year), with spear-phishing the most prevalent identifiable initial infection vector.

ICS-CERT noted that in 2015 it "responded to a significant number of incidents enabled by insufficiently architected networks, such as ICS networks being directly connected to the Internet or to corporate networks, where spear phishing can enable access." Spear phishing and a lack of 'air gapping' between industrial and business networks were both involved in one of the most widely reported IoT incidents so far this year—the downing of Ukraine's power grid.

Incidents like the Ukraine power grid attack, and those on Japan's critical infrastructure described in Cylance SPEAR's February Operation Dust Storm report, are often attributed to nation states. Several pundits also noted the likelihood that terrorist groups will target the industrial IoT.

Other IoT security predictions for 2016 centred on connected cars, smart homes, wearables, medical devices and drones. Unfortunately, Trend Micro's prediction that "At least one consumer-grade smart device failure will be lethal in 2016" came to pass in May when a Tesla Model S's autopilot failed to detect a white tractor trailer in challenging lighting conditions, leading to a fatal collision. This was a malfunction rather than a hack, but there have been plenty of proof-of-concept demonstrations of hacks on connected cars and other IoT devices.

CXO issues

Several security experts noted the rise of cybersecurity from an IT-level issue to a boardroom concern, predicting an expanded role for CISOs (Chief Information Security Officers), in particular, in 2016.

Another prediction, from Trend Micro, that less than 50 percent of organisations will have a Data Protection Officer (DPO)—a requirement of the EU General Data Protection Regulation, adopted in April—in place by the end of 2016 looks likely to hold, given that a recent study estimated that some 28,000 DPOs will need to be recruited (24,000 in the private sector, 4,000 in the public sector) before the GDPR comes into force in May 2018. The UK's 'Brexit' vote in June may have muddied the data protection waters, but it's likely that companies wanting to do business in the EU post-Brexit will still have to adhere to GDPR rules.

An ongoing cybersecurity skills shortage in 2016, cited by both Blue Coat and Vectra Networks in the TPR roundup, is supported by data from ESG's 2016 IT spending intentions survey, which found that 46 percent of organizations claim that they have a problematic shortage in this area (up from 28 percent in the 2015 survey):

ESG went so far as to describe this finding as "a state of emergency"; the survey also found that one-third of respondents have the biggest need for cloud security specialists.

Most security breaches exploit human frailties at some point or other, usually in the early stages of network access, which is why several pundits in the TPR roundup stressed the need for CIOs to educate their user populations on good security practice in 2016—"You can't patch users but you can educate them," as Varonis put it. Given that accidental loss remains the second highest source of breaches after malicious insiders (see earlier), this seems eminently sensible.

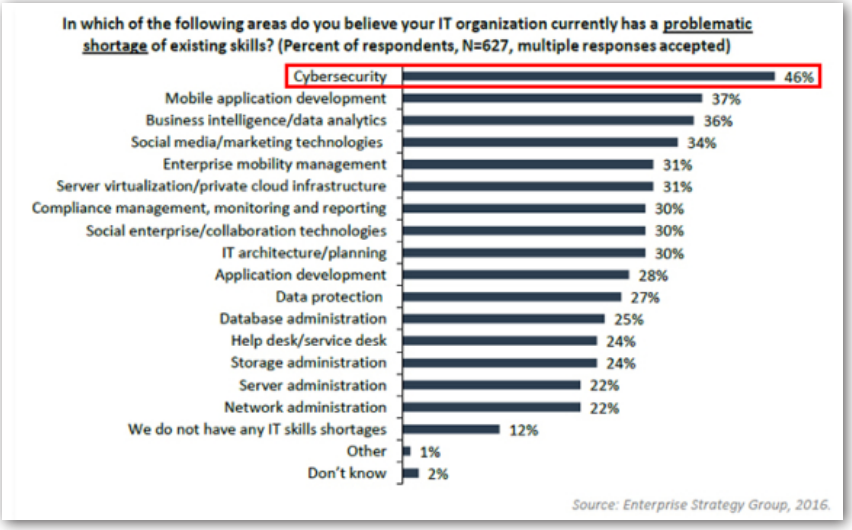


Image: Enterprise Strategy Group (ESG)

Another Varonis prediction for 2016, that "At least five more C-level executives will be fired because of a data breach," will take more time to play out. However, if past form is any guide, more CxOs will indeed walk the plank this year following high-profile breaches at their organisations.

Politically motivated cyberattacks

The main political event of 2016 is the ongoing (and to many outside observers never-ending) U.S. presidential election campaign, and security experts including Varonis, Experian and Raytheon were alert to the hacking possibilities at the turn of the year. And so it has proved, with the theft—and subsequent exposure on WikiLeaks in July—of some 20,000 emails and 8,000 attachments from the Democratic National Committee (DNC). The DNC breach, claimed by a hacker known as 'Guccifer 2.0', has been attributed to Russian intelligence groups—an aspersion denied by the Russian government.

We've already mentioned cyberterrorism in the context of critical infrastructure IoT hacks, and several pundits noted the possibility of increased activity in this area. Security experts also foresaw an increased incidence of state-sponsored and hacktivist attacks during 2016, although this has yet to show up convincingly in the Breach Level Index figures examined earlier.

A note of optimism in this area was provided by LogRhythm, which predicted a rise in 'ethical hacking' in 2016: "More organizations, like Anonymous, will be leaving the dark side and hacking for the public good. They are more motivated by the notoriety and publicity on social media than for financial gain." So far this year, though, the main hack attributed to Anonymous was the attack on the Philippines Commission on Elections in March, which was not noticeably philanthropic.

Mobile security

The rise in mobile payment systems such as Apple Pay, Android Pay and Samsung Pay resulted in several security-related predictions at the turn of the year, exemplified by Raytheon, which noted that "Mobile wallets and new payment technologies will introduce additional opportunities for credit card theft and fraud." In March, researchers demonstrated that stolen credit card details (easily obtainable on the 'dark web') could be uploaded to Apple Pay and security checks from some banks evaded—loopholes that were not found in either Google's or Samsung's systems. Nevertheless, IT governance body ISACA believes that the inherent advantages of mobile payment systems—including tokenization, device-specific cryptograms and two-factor authentication—will reduce risks and increase consumer confidence over time.

While Android remains far ahead of Apple's walled-garden mobile OS in terms of the volume of malware, iOS has certainly seen plenty of security-related headlines this year.

Back in December, Sophos asked "Will 2016 be the year iOS malware goes mainstream?". While Android remains far ahead of Apple's walled-garden mobile OS in terms of the volume of malware, iOS has certainly seen plenty of security-related headlines this year—most notably around the recently discovered trio of zero-day vulnerabilities nicknamed 'Trident' by security researchers Lookout and Citizen Lab. Trident is used in a sophisticated spyware product called Pegasus, which Citizen Lab has identified as the work of a secretive Israeli company called NSO Group.

Elsewhere in the iOS ecosystem, CERT UK and Lookout noted a "huge spike" in malicious activity during the latter half of 2015 thanks to SDK-exploiting malware such as XcodeGhost, resulting in a heightened background level through Q1 2016:

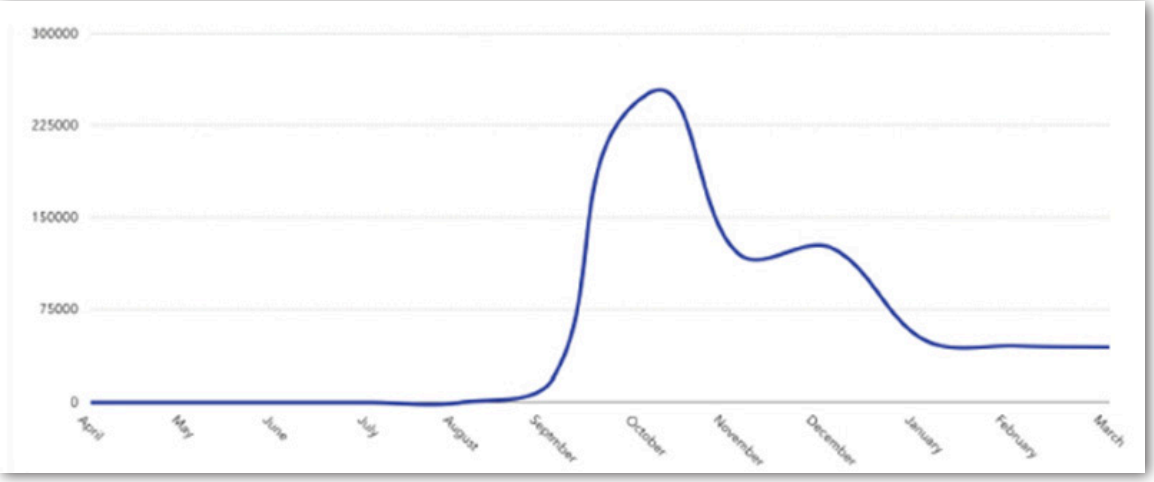


Image: CERT UK/Lookout

Although iOS is clearly vulnerable to sophisticated targeted attacks and malware introduced via the App Store, Android remains the more generally exposed platform, as this chart from the aforementioned CERT UK/ Lookout report shows:

Image: CERT UK/Lookout

Mobile malware is certainly still on the increase. In Q1 2016 alone, CERT UK saw 48 percent of the full-year 2015 amount of unique mobile malware samples, broken down as follows: chargeware (31%); adware (26%); trojans (20%); riskware (15%); spyware (7%); other (1%).

Finally, DomainTools may have been prescient in December when predicting "A rise in botnets running on mobile devices...we believe that 2016 will see an inflection point, with a marked increase in mobile botnet activity." This year has seen the discovery by Check Point of the Viking Horde malware that infects Android phones via Google Play apps, and also the first trojan that uses rogue Twitter accounts rather than traditional command-and-control (C&C) servers to co-ordinate infected devices.

Cloud security

As companies increasingly store ever more valuable data in the cloud, so the 'bad guys' will inevitably follow. That's why, back in December, Blue Coat expected to see "An increase in breaches of cloud services" in 2016, with hackers using credentials to cloud services as a major attack vector. Furthermore, said Blue Coat, "social engineering tactics will focus on mimicking cloud login screens to gain credentials."

An important point here is that credential theft is more common than breaches of the cloud services themselves, which is why ThreatStream predicted that 2016 would be the year when "credential exposures reach a tipping point that causes some major cloud providers to force multi-factor authentication for all users."

DataVisor also drew attention to the use of cloud services to launch cyberattacks: "Businesses and consumers are not the only ones moving to the cloud. In 2016, we expect to see the continued migration of cyber attack infrastructure to the cloud, as cloud services become more pervasive and cost-effective. Cloud services such as AWS, Azure and Google Cloud are already victims as fraudsters register a massive number of free,

trial accounts and use their computation infrastructure to conduct attacks."

Other notable cybersecurity trends in 2016

Beyond the top five trends identified in Tech Pro Research's January article, *ransomware*—which came in at number seven—has had a lot of visibility so far this year.

Hospitals and other medical institutions have been a particular focus for ransomware attacks this year, mostly targeted at patient records and other vital data. We've yet to see ransomware targeted at a "medical device or wearable", as predicted by analyst firm Forrester, but the likelihood remains high that this will happen at some point.

Encryption—number 14 in TPR's prediction list—has had a lot of airtime this year, thanks mainly to Apple's well-publicised spat with the FBI over the encrypted contents of one of the San Bernardino shooters' iPhones.

Vectra Networks' prediction that 2016 would see ransomware "focus more on holding enterprise assets hostage and less on individuals," is supported by a recent report from Malwarebytes, which found that nearly 40 percent of businesses surveyed (from the US, Canada, the UK and Germany) experienced a ransomware attack in the last year, with over a third of affected enterprises losing revenue, and one in five (20%) having to cease business completely.

Encryption—number 14 in TPR's prediction list—has had a lot of airtime this year, thanks mainly to Apple's well-publicised spat with the FBI over the encrypted contents of one of the San Bernardino shooters' iPhones.

A specific encryption-related prediction, from A10 Networks, that "attacks hidden in SSL traffic will exceed attacks in clear text", has recently been followed up with a survey (conducted in partnership with the Ponemon Institute). Key findings included 80 percent of organisations (from North America and Europe) suffering cyberattacks in the past year, 41 percent of which used malware hidden in SSL traffic to evade detection. Only 36 percent of respondents believed they could detect malicious SSL traffic, which is likely to increase (both inbound and outbound) over the next 12 months. The performance hit involved in decrypting and inspecting SSL traffic was the overwhelming concern for the organisations surveyed.

Finally, although ***analytics and cyber-threat intelligence*** made a good showing at the turn of the year, making number 11 in TPR's chart, we might have expected more specific predictions about the use of AI and machine learning in cybersecurity. As a specialist in this area, it's no surprise that Vectra Networks believed "organisations will realise that algorithms - not Big Data - are the key to detecting and mitigating active cyber attacks."

Perhaps the most interesting AI/cybersecurity event so far this year was the DARPA Cyber Grand Challenge (CGC) at this year's DEF CON/Black Hat conference in Las Vegas. Designed to foster the development of advanced, autonomous systems that can detect, evaluate and patch software vulnerabilities before the bad guys can exploit them, the CGC involved seven competing teams including white-hat hackers, academics and private-sector cybersecurity experts. The winning team, Pittsburgh PA-based ForAllSecure, took home a $2 millon prize.

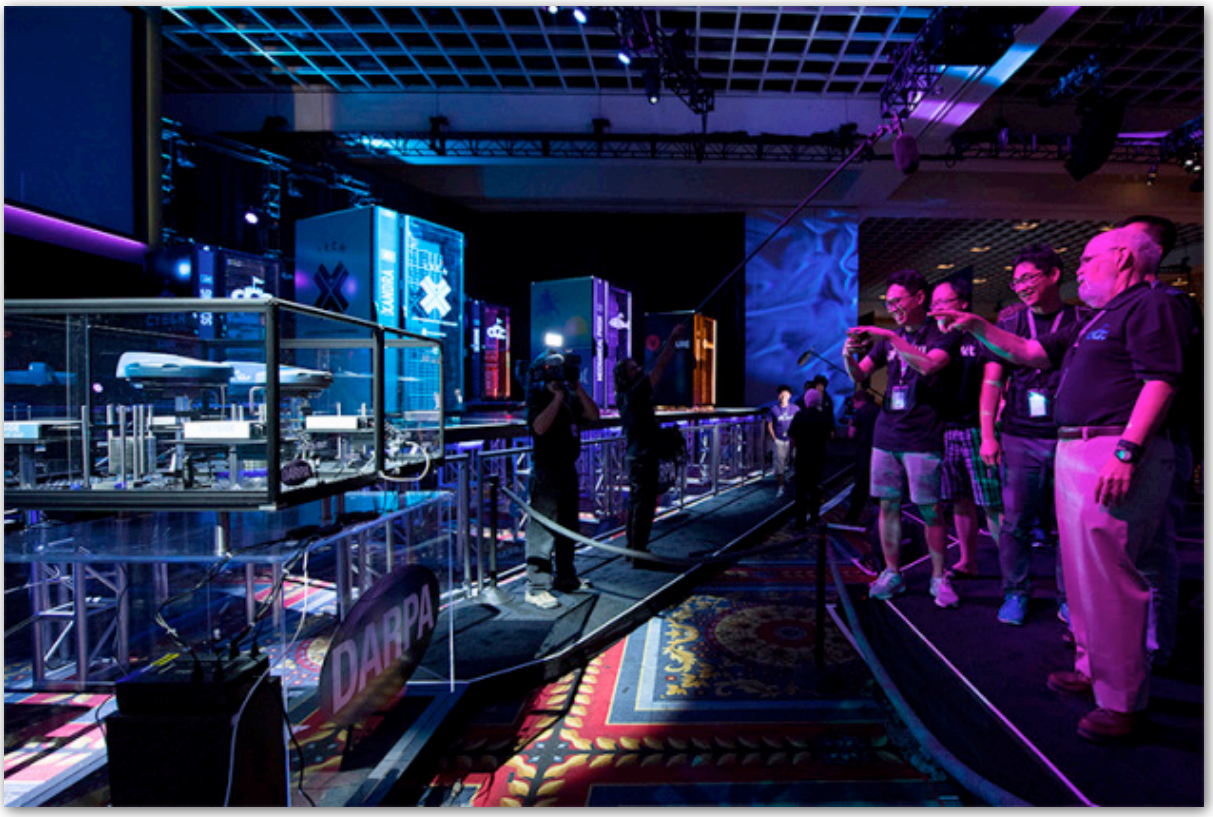


Image: DARPA

Additional resources

Governments and nation states are now officially training for cyberwarfare: An inside look

Europe, Canada, USA, Australia, and others are now running training exercises to prepare for the outbreak of cyberwar. Locked Shields is the largest simulation and TechRepublic takes you inside.

Download the PDF.

Research: Companies fear mobile devices as massive cybersecurity

According to an online poll conducted by Tech Pro Research in June, everyday threats like security breaches involving mobile devices are more worrisome than acts of cybercrime. More results from this research are presented in the infographic below. To learn more, download the full report, Cybersecurity Research: Weak Links, Digital Forensics, and International Concerns. (Tech Pro Research membership required.)