

# A STEP AHEAD

FOCUS ON SECURITY

IN THIS ISSUE:

HOW MCAFEE UNCOVERED  
A CYBERCRIME GANG AND  
AIDED IN THEIR ARREST

THE FUTURE OF  
CYBERSECURITY

BIG THREATS, CRITICAL  
MOVES & ONGOING TRENDS

WHAT WE SHOULD AND  
SHOULD NOT DO IN 2018

INSIGHTS AND TIPS FROM  
THE WORLD'S MOST FAMOUS

**FORMER**  
**HACKER**



SET THE PAGE FREE

# Think you're secure?

## Why you may be surprised.

With more than 50,000 security threats emerging each day, IT managers like you have a challenging job. Even with carefully crafted policies, the biggest threat may come from inside your organization. Firewalls, antivirus software, rules and regulations can only do so much. The final barrier is employee behavior and, when you're waging the war against laid-back attitudes, culprits can be everywhere.

### Did you know?



# 98%

of compromises took just **minutes**, or less, to perpetrate.<sup>1</sup>



Intellectual property (IP) theft has reached "unprecedented" levels, costing the U.S. an estimated **\$300B** a year.<sup>2</sup>

### Who's ignoring the rules?

87% of employees work at a company that has an IT security policy.

**However:**

**1 in 10** rarely or never follow the policy.

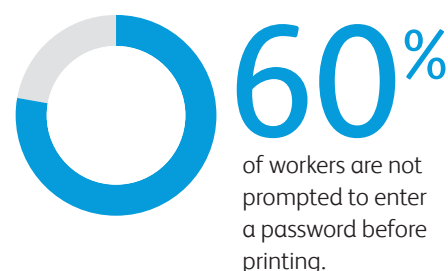


**1.5 in 10** are not aware of what the security policies are.



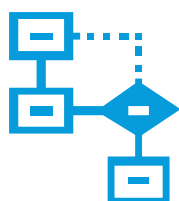
Over half of U.S. employees who print, scan or copy confidential information never, or rarely, worry that those items will remain secure.

### Why you should be worried:



### What can you do?

With the right balance of people, processes and technology, you can protect sensitive data wherever it resides.



Make your IT security policy more than a written document. Communicate the 'how' and the 'why' regularly and require your policy to be part of day-to-day procedures through supporting technology.

Nothing does more than a proactive approach to policy awareness and adherence. When you think you've kicked worry to the wayside, think again. The threats are all around and always changing. And security is everyone's responsibility.

For more about how Xerox can help, visit [www.xerox.com/security](http://www.xerox.com/security).

Source: Online survey conducted within the United States by Harris Poll on behalf of Xerox, between May 7–11, 2015, among 2,013 U.S. adults, ages 18 and older.

1. Healthcare Threat Landscape: [http://www.verizonenterprise.com/resources/factsheets/fs\\_dbir-industries-healthcare-threat-landscape\\_en\\_xg.pdf](http://www.verizonenterprise.com/resources/factsheets/fs_dbir-industries-healthcare-threat-landscape_en_xg.pdf)

2. The commission on the theft of American intellectual property, 2013

©2015 Xerox Corporation. All rights reserved. Xerox® and Xerox and Design® are trademarks of Xerox Corporation in the United States and/or other countries. 11/15 COLKA-145 BR17012 SECPT-01UC

# A Positive View on the Future



## MIKE FELDMAN

Executive VP and President,  
NAO, Xerox Corporation

### 2017 WAS QUITE A YEAR. IT WAS, FOR MANY, A WAKE-UP CALL.

Equifax, one of the largest credit bureaus, fell victim to hackers who stole the personal data of 145 million people, including social security numbers. Questions still abound regarding that attack, such as who was behind the hack, what will the impact be, are data brokers doing enough to keep information secure?

In October, we learned that every one of Yahoo's 3 billion accounts was hacked in 2013 – three times what was first thought when the company first learned of the breach in 2016. They too do not know who was responsible.

Government tools were leaked by the Shadow Brokers. Hospital systems were hacked.

Voter records were exposed. School districts were targeted. WannaCry, Bad Rabbit, The Dark Overlord became familiar names.

These cyberattacks and more point to the increasing vulnerability of our information.

As the cybercriminal industry becomes more mature, tools such as malware and ransomware become more pervasive and more malicious. And we can expect more of this in 2018. It is predicted that the Internet of Things will keep hitting multiple industries as they rely more on smart technology.

And yet, I remain optimistic, confident and excited for 2018. Our future has never been more exciting. As innovative services and technology break down barriers and present opportunities, we face a future in which we can be more productive, more connected and more informed than ever.

In this issue, you'll find positive insights on what's happening today to keep information safe, and what future trends are. I'm particularly fascinated by recurring themes such as collaboration and interoperability.

In the pages ahead, you'll learn:

- How to keep your business-critical information safe through the eyes of the world's most famous (former) hacker, now on the right side of the fight.
- Enterprise-wide best practices that ensure personal information and private business data stays confidential.
- Who's doing what to protect your network and your documents, including new capabilities embedded in office technology through partnerships with McAfee and Cisco.

The purpose of this magazine is not to alarm, but to inform and inspire, keep you optimistic about the future of technology and the role it plays in the continued growth and profitability of your business, **and free you and your organization from security risks.**

The future of business has never been more exciting as we are presented with new opportunities, new tools and new innovations every day.

A handwritten signature in black ink, appearing to read "Mike Feldman".





# Table of Contents

**6**  
**KEVIN MITNICK, THE WORLD'S  
MOST FAMOUS (FORMER) HACKER**  
proves you're more vulnerable than you think.

**12**  
**WHAT DRIVES INDIVIDUALS  
TO CYBERCRIME**  
and how can we stop them?

**16**  
**THE FUTURE OF CYBERSECURITY**  
by Dr. Alissa Johnson, Chief Information  
Security Officer, Xerox

**18**  
**Q&A WITH DOV YORAN**  
Sr. Director, Strategy & Business Development,  
Security Business Group for Cisco Systems, Inc.

**20**  
**A CHANGE IN MINDSET FOR  
A SHIFTING LANDSCAPE**  
Sergio Caltagirone, Director of Threat Intelligence  
and Analytics of Dragos, gives us his take.

**24**  
**RETHINKING THE SECURITY OF  
IOT SYSTEMS**  
by Ersin Uzun & Shantanu Rane, System Sciences,  
Laboratory, PARC, a Xerox company



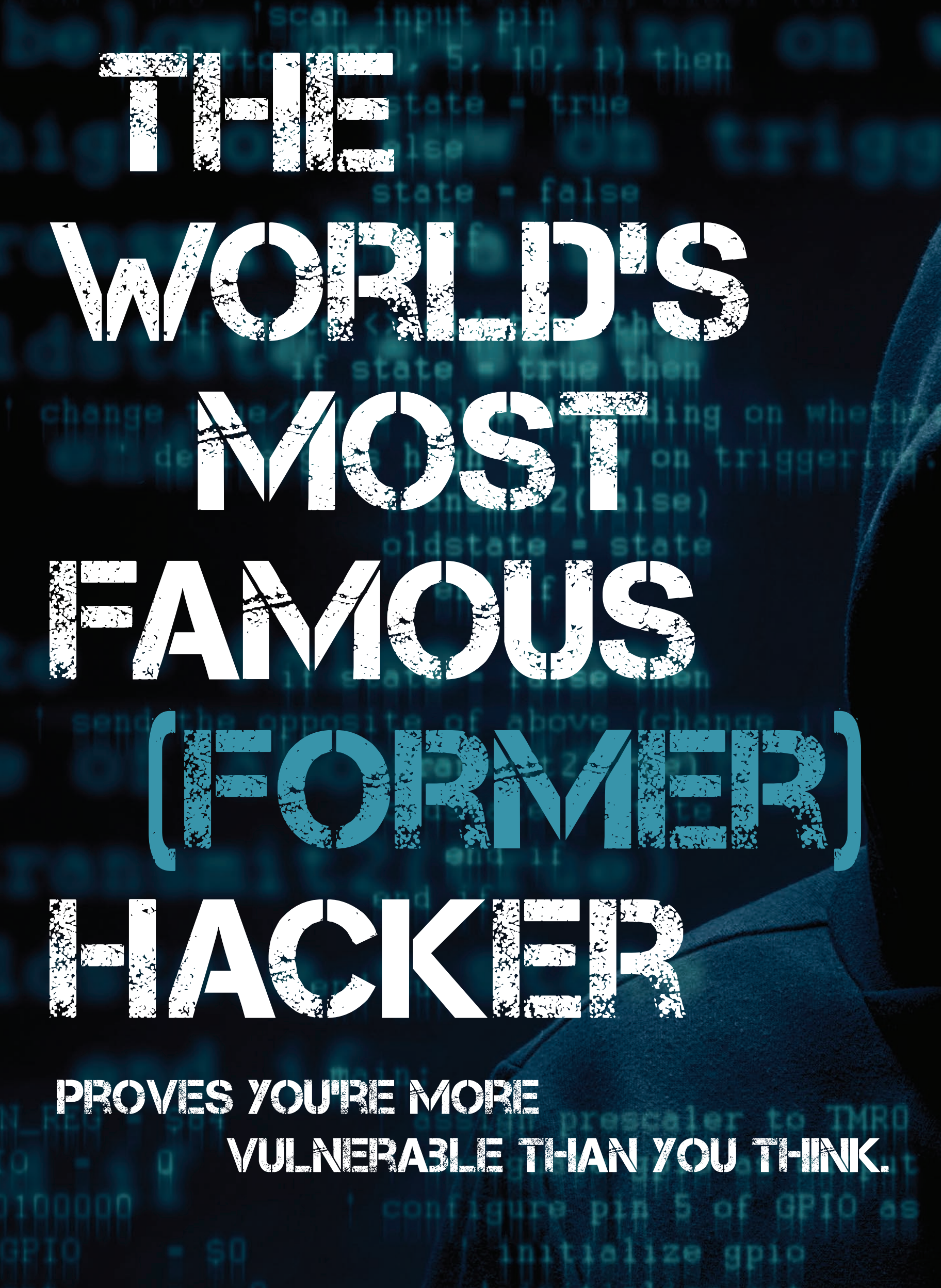
# Cyber Criminals and Bad Actors Beware

Meet the Super Cyber Squad: The unstoppable, fearsome foursome dedicated to keeping security threats unseen and inert, your offices safe and your vital information untouched — thanks to unbeatable intrusion prevention, device detection, document and data protection and partnerships forged on your behalf. Cybercriminals and bad actors beware. The Super Cyber Squad has its sights set on you.



Your office environment and vital information are safe with us.





# THE WORLD'S MOST FAMOUS (FORMER) HACKER

PROVES YOU'RE MORE  
VULNERABLE THAN YOU THINK.





```
lngCounter = lngCou  
if lngCounter = 11377 Then '/// c  
    secs = secs + 1 '/// i  
    lngCounter =  
    end if  
    if secs = 60 then  
        secs = 0  
        minutes = minu  
        end if  
        if minutes = 10  
        if state = blnAlarm  
        STILL in the 'alarm'  
        '/// signal every  
        transmit(blnAla  
        end if  
        end if  
        = 60 then  
        hours = hours  
        minutes =  
        end if  
        STILL is  
        if state = blnAlarm  
        if (blnAlarmSignal  
        transmit  
        else  
        transmit  
        end if  
        oldstate =  
        input
```



# THE WORLD'S MOST FAMOUS (FORMER) HACKER



## KEVIN MITNICK

Kevin Mitnick is the world's most famous hacker, bestselling author, and the top cybersecurity speaker. Once one of the FBI's Most Wanted, he is now a trusted security consultant to the Fortune 500 and governments worldwide. His books include "The Art of Intrusion: The Real Story Behind the Exploits of Hackers" and "Intruders and Deceivers and The Art of Deception: Controlling the Human Element of Security," which are mandatory readings for security professionals. His autobiography, "Ghost in the Wires: My Adventures as the World's Most Wanted Hacker," was a New York Times best seller and his latest work released in February 2017 is a groundbreaking book on privacy, "The Art of Invisibility."

It's a typical morning at a leading health care clinic. Nurses are buzzing about, doctors are making their rounds, patients are dining on their choice of oatmeal, scrambled eggs, or toast and jam.

In between replenishing supplies and checking vitals, a nurse receives an email from HR with a holiday schedule update and a link taking her to a chance to be one of 15 lucky winners of a Fitbit.

Woohoo, she thinks. Holiday season is starting off right.

Except the email isn't really from HR. It's from Kevin Mitnick and his team, who were hired to conduct penetration testing to identify holes in the organization's security ecosystem. And the link she clicked to take her to the entry form also fired off a macro document that deployed and installed malware on her computer.

The damage didn't stop there. Once Kevin's team was able to hack the victim's workstation, they continued with a multi-step technical exploitation process that yielded administrative rights across the entire domain within days.

"We gained access to everything," Mitnick says. "All financial records, all patient records, everything. And we were there for two months before they detected us."

That's because the organization had what Mitnick calls, "M&M Security," as in hard and crunchy on the outside, which makes it difficult to get in, with nothing internally to prevent lateral movement.

"Too many companies focus their security efforts on keeping outsiders out, but don't include the due diligence of ensuring proper configuration, password and patch management," Mitnick says. "It's critical to have a security expert evaluate your environment to ensure best practices and security controls are implemented within your environment. Whether you use in-house security experts or outsource the service, have them evaluate your environment to identify your weak links."

Let this be a lesson for all industries. Attackers use the same methods, whether they're attacking a financial institution, a government agency, a corporate entity or a retail mall.

## EVERY INDUSTRY VULNERABLE

Mitnick and his team are currently testing a North American retailer that uses a cloud service for processing payroll.

"Let's call it payroll.com," he says. "This particular company is headquartered in a different country. Let's say Mexico."

The payroll company only bought and registered payroll.com, so Mitnick bought the domain payroll.mx and set up a clone of the real payroll site.

"It looks exactly the same," Mitnick says. "All we had to do was call the payroll administrator pretending to be IT, asking him to go to payroll.mx to log in because the cloud provider wanted customers to use their country domain for expediency, as the servers would be closer in geographical proximity."

The administrator had no reason to doubt anything – the site looked exactly like the site he was used to. "We were able to deploy a SSL certificate for the fake site, enabling us to gain trust and credibility," Mitnick says. So, the administrator followed along. Mitnick then prompted him to enter all his credentials, which he did.

"In that instant, I had full administrative access to the payroll for the entire company," Mitnick says.

It took less than 10 minutes.

## ALSO, BE WARY OF THE PHYSICAL BREAK-IN

Mitnick and his team also do physical security testing, pinpointing ways bad

actors can bypass access card security controls to get inside a customer's facilities. For example, one client had fingerprint readers for building access.

"In this case, the readers were not properly configured with a tamper switch, so we had the opportunity to take the reader off the wall and install a malicious hardware implant," Mitnick says. "Then, when legitimate employees signed in with their biometrics, we were able to connect via Wi-Fi with our mobile phones and replay the data to open the door. Once we gained access to the building, we gained the ability to compromise laptops and workstations."

The cybersecurity landscape is filled with organizations that have been hacked like that. There is no computer, no IoT device, no reader that cannot be hacked. In fact, the smarter the refrigerator, the thermostat, the lighting, the more vulnerable it is. Or, as Mitnick likes to say, "The more complexities built into the technology, the more vulnerabilities."

So, what is one to do?

### BE PROACTIVE VS. REACTIVE

Understand the threats that you face as a business and a consumer, and know how to mitigate the risk as much as possible.

"The first step is doing a risk assessment of your environment," Mitnick says. "Look at what could be considered the low-hanging fruit, then employ security controls to mitigate risk," he says.

But the best advice, he adds, is to get a security expert internally or externally to deploy best security practices.

"Hire someone to do penetration testing. Get an accurate snapshot of your security. Discover where your security controls fail, and then, once you do this exercise, have the road map for what you need to do next; what steps you need to take to secure your environment."

### TRAIN YOUR PEOPLE TO STOP, LOOK AND THINK

Every organization is a potential victim of social engineering attacks that could appear to come from a supplier, a vendor, a customer or an internal employee.

"Educate and train your people to recognize them by using the same sources and methods the adversaries use," Mitnick says.

He suggests you consider using a company like KnowBe4 to conduct simulated phishing to inoculate your organization against the real bad guys.

"The goal is to train users to make smarter security decisions, and to stop, look and think before clicking a link or opening an attachment or giving out sensitive information."

Final words of advice: Assess your situation. Do your homework. Remember that we're all in this together. And last, find partners you can rely on who take your security as seriously as you do.

## SIX STEPS TO MITIGATE RISK IN 2018.

- 1. Be proactive** rather than reactive. Keep up to date with recent security threats that could affect your business.
- 2. Understand the threat** facing you as a consumer and in your business. Get a snapshot of your security and mitigate the risk to the highest degree possible.
- 3. Do a risk assessment** of your environment. Set up a pen testing schedule and consider using a bug bounty to reward people who report security vulnerabilities on your internet-facing website and/or any of your company's external network resources.
- 4. Make sure your operating system is up to date.** For example, if you're running Windows 7, even if you have all the patches for the latest security flaws, you will never have the level of security features that Windows 10 has.
- 5. Employee security awareness training.** Test to see if they fall for a phishing attack.
- 6. Make sure all internet-facing websites and network services, including cloud services, are properly secured,** and that remote access requires two-factor authentication.





COMPANIES USE UP TO

50

DIFFERENT  
SECURITY VENDORS.  
HOW MANY IS TOO MANY?

*There's never been a better time  
for security that works together.*





# The Protector:

**FAVORITE PHRASE:** Just try and get past me.

**SUPER POWER:** Protection

**SPECIALTY:** Protecting printed and scanned documents from compromise.

The Protector drills deep to prevent the deliberate or accidental transfer of key data to those not authorized to see it.

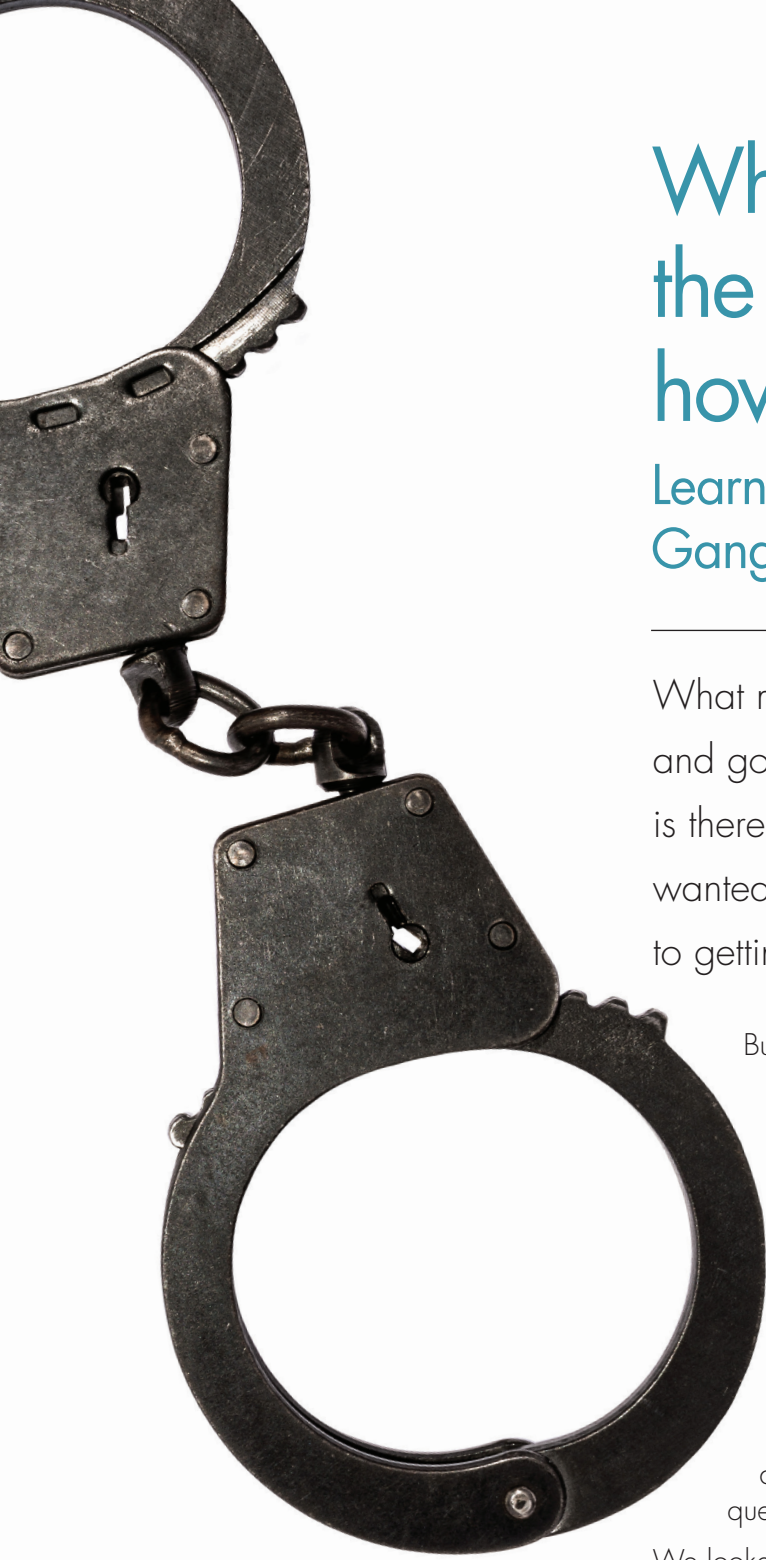
He's an encryption Jedi master, well-versed in National Institute of Standards and Technology (NIST) and U.S. Department of Defense approved data clearing and sanitization algorithms.

Your office environment  
and vital information  
are safe with us.



SET THE PAGE FREE





# What drives individuals to join the world of cybercrime, and how can we stop them?

## Learn How McAfee Uncovered a Cybercrime Gang and Aided in their Arrest

What motivates cybercriminals to target and attack corporations and government entities? The obvious answer is money. However, is there more to it than that? As a cybersecurity company, we wanted to know, and we took a unique, straightforward approach to getting this answer: we asked the cybercriminals themselves!

But first, how to find them? We could go into forums and look for these individuals, but this would be time-consuming and odds were slim that we would find the right person. So, we took samples of recent ransomware and examined the ransom note, which like most notes contained an email address where to send your payment and even a help desk type of email address for questions.

We looked at months of unique ransomware samples and extracted either the images or the notes that contained the contact addresses. As new ransomware families popped up in our tracker, we verified them and added the addresses — because fresh attacks made it likely the authors would interact with us.

After accumulating these addresses, we sent emails asking if they would answer a few questions. Interestingly enough, when we sent these emails, we found that 30 percent of the addresses were either fake or nonexistent. So, in these cases when files were encrypted and the victim decided to pay, using email to send

evidence of payment was useless. The money was gone (as well as the files).

During the first week of research, we received answers from some of the actors, but most were not willing to cooperate. That's no surprise: They were cautious about revealing their identity.

During the second week, we had better luck and started to chat with a few. That number grew, and after a few weeks we had a great collection of conversations going.

### **"FAST, EASY AND SAFE"**

When we asked why they started a career in ransomware, most answered with variations of "enough money" and "fast, easy and safe," especially when using anonymous email services and cryptocurrency for payments.

### **HOMEMADE VS. OFF THE SHELF**

Most of the actors we spoke with wrote their own ransomware. They had looked at published source code, but were clever enough to come up with their own variants that contained new techniques or different approaches to keep detections low. The longer they stayed out of sight of endpoint security solutions, the longer their opportunity to make money.

```
You must pay 550 $ via BTC for the decryption key
You have 4 days to pay for my services. After this period, you will lose all your files.
Step 1 - Create an account www.localbitcoin.com
Step 2 - Buy bitcoin worth 550 USD
Step 3 - Send the amount to this address: 1F6nfAKenZvzS*****
Step 4 - Contact us on this email: *****@gmX.com with subject: DECRYPT KEY FOR ID-CLIENT-*****
After these steps you receive a software + key and tutorial for decryption.
For any questions please contact us at this email address: *****@gmX.com
```

An example of ransomware.



## SPENDING THEIR ILL-GOTTEN GAINS

We found that they spent the revenue gained from their campaigns in various manners: travel, cars. One responder had many affiliates working for him and was planning to buy a house. One of the most surprising answers was to “pay off debts.”

## WILLING TO NEGOTIATE

Although they often have the image of being ruthless, almost all of them claimed a willingness to negotiate the ransom price if the victim could not afford to pay the demanded amount.

## TRACKING THE AUTHORS

One of the actors told us he not only sends ransomware, but also sells botnets and other fraud-related services. He was open to sharing more information, so we kept the conversation going. We learned he was not a very experienced actor since he gave clues to his whereabouts. In one of the conversations, he shared some examples, but the data was not scrubbed. By correlating the data he provided with other information, such as email time zones and mistakes in his English, we traced him to Dakar, the capital of Senegal, in West Africa.

## AN EYE-OPENING EXPERIENCE

One of the interesting findings was that cybercriminals have a sense of absolute safety when conducting criminal operations. Cybercrime is a crime like no other, perceived as low-risk with high returns, which contributes to its rapid growth.

However, this is misguided thinking. Law enforcement agencies around the world are teaming up with academic institutions and cybersecurity companies, including McAfee, to take down these individuals.

In 2016, a massive spam campaign struck the Netherlands. Files were encrypted and ransom notes appeared. The Dutch High Tech Crime Unit began an investigation and requested the help of McAfee's Advanced Threat Research team to assist in identifying samples and answering questions.

We were able to determine that the criminals behind the Netherlands campaign were also responsible for spreading ransomware throughout Europe and the U.S.

Most importantly, we were able to determine these actors were operating in Romania.

## THE ARRESTS

In mid-December 2017, Romanian authorities stormed into the houses the suspects were working in and arrested three individuals for allegedly spreading CTB Locker ransomware. During this law enforcement operation called “Bakovia,” six houses were searched, whereby the investigators seized a significant amount of hard drives, laptops, external storage, cryptocurrency mining rigs and hundreds of SIM cards. In a parallel ransomware investigation, two other suspects from the same criminal group were arrested at the airport in Bucharest.

This law enforcement action emphasizes the value of public-private partnerships and underscores the determination behind the McAfee mantra, “Together is power.”

*(Continued on next page)*

# Never pay the ransom

To reduce your risk of picking up ransomware: Keep your OS, security and application software up to date; regularly back up data stored on your computer; exercise a healthy dose of skepticism even when you see messages that appear to come from legitimate sources; and do not click on links or open files from unknown names or organizations.

**>> If you do get infected, don't pay the ransom <<**

As we saw with our research, it most likely will not get you your files back. Plus, your payment will help fund the cybercriminals' next attack.

Report the infection to the authorities and visit [NoMoreRansom.org](http://NoMoreRansom.org) to see if a decryption tool is available.



# What drives individuals to join the world of cybercrime, and how can we stop them?

(continued)

## CTB LOCKER

CTB Locker, also known as Critroni, is known as one of the largest ransomware families — helping to drive a new ransomware surge of 165 percent in 2015, and earning a spot as No. 1 just a year later. Operation Tovar, in which law enforcement agencies took down the infrastructure responsible for spreading CryptoLocker, created a need for more malware — CTB Locker and CryptoWall malware families helped to fill the gap.

In June 2014, the CTB Locker authors began to advertise the malware family on the underground scene at a cost of \$3,000USD, where people could buy the first versions for \$1,500USD. The authors also offered an affiliate program, which made CTB Locker infamous. By sharing a percentage of the received ransoms, the affiliates ran the greater risk — because they had to spread the ransomware — but they also enjoyed the higher profits. By using exploit kits and spam campaigns, the malware was distributed all over the world, mostly targeting “Tier 1” countries, (those in which the victims could afford to pay and most likely would pay the ransom). Midway through 2015, we gained unique information from an affiliate server that helped us tremendously in the subsequent investigations.

HomePrice rulesPayoutsStatsInstallsGet EXESupportUser messagesAPI

Show all

SubID	Count
0	254
22	4
31	102
1209	134
1211	407
1311	282
1411	126
1511	154
2211	190

N	Reported	Last active	Installation ID	Mode	V	OS	CC	TZ	Geo	SubID	Files	Address for payment	Price	Paid
1830	10/12 15:20	08/01 15:16 W	c40b7217f948e4b6	GUI	2.4	6.1.x64 H	TW	+8	TW	1209	8=0MB	1952N5W7XpaNo8p6CNDyXNFRk63nk(B6eM	0.6	0.6
1458	24/11 10:59	27/11 17:08 WD	8ee2fb382041b1eb	GUI	2.3	5.1	PL	+1	PL	2211	7848=44.5GB	1ExApRqmCyn4eMV68eJ48TChp1zzWtzS2	0.6	0.80046147
434	12/11 00:44	12/11 17:07 N	1b4960440d4dc12e	GUI	2.2	6.1	AU	+10	AU	1211	63827=19.9GB	1KdeqBij3erwtFSDDC8Pa9KL72KztD9Rf	0.6	0.6
410	11/11 23:54	14/11 12:50 WD	cbb42be8414d003f	GUI	2.2	6.2.Srv	PT	+0	PT	1211	34797=30.9GB	1KfoB86GZK3x9qtfPacVob2kwFt4eyMDV	0.6	0.6
341	02/11 08:29	07/11 05:21 WD	e89984c7e3427395	GUI	2.2	6.1.x64 H	+8	TW	31	821=30.3GB	1Hc8Bw5AbB3GHy2IAND8GecEb9Nmm3J	0.6	0.6	
152	28/10 18:49	30/10 05:15 W	5e2f198e4b42940d	WEB	2.2	6.1.x64 H	+8	TW	0			1BY2MeK9RCJTWU3eipD6BC8Qx4eKdhQQCm	0.5	0.5

Last active hints:  
G - GUI with direct TOR connection  
N - NoTOR or GUI via tor2web proxy  
W - manual webpage via Tor Browser  
D - decoded test file via Tor Browser

OS hints:  
L - Low integrity level.  
M - medium/user level  
H - high/admin/system level  
V - virtual machine. Usually bad/AV with exception of VDS

A CTB Locker affiliate server. In addition to an affiliate server in CTB Locker’s infrastructure, two other components complete the setup: a gateway server and a payment server.

```
if (isset($_POST["decrypt"])) {
    $req = "vic";
    socket_write($sock, $req, strlen($req));
    $req = str_pad($_POST["domain"], 128);
    socket_write($sock, $req, strlen($req));
    $resp = socket_read($sock, 64);
    if ($resp == "not_paid") {
        echo json_encode(array("status" => "not_paid"));
    } else {
        echo json_encode(array("status" => "success", "decrypt" => $resp,
            "dectest" => $dectest,
            "secret" => substr(md5("djf33".$_POST["domain"]), 2, 10));
    }
}
```

An example of CTB Locker source code.

This info came from: <https://securingtomorrow.mcafee.com/mcafee-labs/advanced-threat-research/>

# The Detector:

**FAVORITE PHRASE:** Wherever you go, I'm there.

**SUPER POWER:** Device detection

**SPECIALTY:** Detecting harmful changes and stopping malware in its malevolent tracks — before it can do evil.

The Detector is thorough, comprehensive, ever-alert and on the job 24/7. She lives for ferreting out adversaries and evil-doing. She's focused — obsessed even — with singling out people and organizations she perceives to be a threat to the mental and physical health of the world.

Your office environment  
and vital information  
are safe with us.



xerox 

SET THE PAGE FREE



# The Future of Cybersecurity

By Dr. Alissa Johnson, Chief Information Security Officer, Xerox



## **ALISSA JOHNSON, PH.D.**

Chief Information Security Officer for Xerox and the former Deputy CIO for the White House.

How many of us have looked ahead and asked, “What is in the future, and how can we anticipate what’s going to happen?” I am asked that many times as it relates to the future of cybersecurity.

It is as if there were only one future, but there is not. The fact of the matter is, we are not preparing for just one future – the future is an amalgamation of many future aspects. This big future contains the future of breach, the future of economics, the future of ecosystems, the future of politics, the future of privacy and that list goes on and on.

All of these futures play a role in shaping what the amalgamation of futures looks like. All of these futures are continuously moving, shifting and reshaping, which means we need to be flexible enough to move along with the ebb and flow so that all aspects are covered.

Any change in either of these futures changes their trajectory, and every change has a ripple effect on many other aspects. It is also dependent on which breaches and exposures are reported and their ramifications. These impact the future of personal responsibility as well as tolerance.

With this in mind, it is hard to really anticipate what the future of cybersecurity is, but easier to anticipate and prepare for any of these shifts that affect the future. With this level of connection, if we lose track of one aspect, then we will lose track of a critical piece that influences the future. Xerox is decomposing all those futures, and works internally and externally to address security.

### **THE FUTURE IS THE INTERNET OF THINGS**

The Internet of Things (IoT) is changing cybersecurity. Not only do we need to think about connectivity in our homes, but also connectivity in our offices – our printers and smart devices are now more connected externally and open us up for network

exposures. We can now be potentially thought of as an endpoint and have to protect ourselves from being a conduit into the network.

The Internet of Things is also the largest ecosystem with a diverse set of components and thus has a tendency to blur the lines between business and personal data. The goal is not to hinder this sort of innovation but protect the data and compartmentalize it to an extent where usage is acceptable as opposed to shadow environments. We accept the fact that users want more functionality and businesses want less shadow information technology environments, so the enhancement of IoT security is important.

### **THE FUTURE IS LAYERED**

The future is a dynamic, heterogeneous environment with many layers. Each of these layers plays an important role in maximizing the security of the environment.

The first layer is data security. In this layer, we evaluate our data and prioritize it, making our most coveted assets more important over those less meaningful. Those “most coveted” are usually referred to as crown jewels. A king and queen will have their most prized possessions protected by knights, guards, a moat, and may store them in a highly secure location.

Our crown jewels should be protected in the same way. No longer can we provide the same broad-brush stroke security policies across all of our data. It is now necessary to classify the data, prioritize the data and ensure that investments are made proportional to the value of the data.

The second layer is application security. Our applications must securely handle the data to prevent leakages and exposures. Applications have essentially become a conduit to carry and process data outside of our typical network boundaries. We must encourage secure coding practices and secure data processing.

The third layer is infrastructure security, which focuses on the hardware. Vendors are always enhancing the security of their products. We must accept those enhancements and integrate them into our operational infrastructures. As a participant in the vendor population and a consumer of goods, Xerox takes a simplified approach. We have partnered with key security vendors to ensure that we easily integrate into our customers' environments.

The last layer are our security processes. This includes processes and policies. The adversary depends on human trust so our policies must protect us. Many times, non-security controls and implementations help to increase the security posture. In this, I am including automation and simplification of our processes, which in turn will have additional benefits with security.

In the end, all of these layers have to be congruent, non-tangential. They have to work together but may not necessarily be presented in a specific order. The goal is to increase harmony in order to influence cohesive security.

### THE FUTURE IS GOVERNANCE-DRIVEN

Culture should not dictate governance; governance should dictate culture. We cannot accept that an organizational culture can push back on security elements such as two-factor authentication or changing passwords. We have to instead look at what is best governance for an industry, for a company and then teach the culture to be accepting. Educating the culture is key, as security is everyone's responsibility.

### THE FUTURE IS PARTNER-BASED

As we focus on each part of our layered architecture, we must include our partners. We are in an arms war which means we need to increase our partnerships and include our partners in our arsenal. Security is really solutions-based as opposed to device specific. A device is a part of a larger infrastructure that integrates with other vendor components. Partnerships are important in ensuring the ease of integration, acceptance of security controls and improving the security posture. It is a team event. The goal is to develop and maintain continuing partnerships to ensure the solutions are more secure and not just the individual components.

Xerox works with compliance-testing organizations and security industry leaders such as McAfee and Cisco to enhance and protect devices with the latest security standards. These leaders also help with integrating into our customers' security architecture and enhancing protections within their environment.

### THE FUTURE IS COGNITIVE

Cognitive processes increase our ability to allow machine learning to enhance security. Right now, we allow engines to analyze data, thus the large focus on data analytics and synthesis. The future extends that in allowing the engines to react and respond based on learning baseline infrastructure behavior. This may be an interesting way

to address the shortage of cybersecurity talent. The more processes that we have to react and address lower level tasks, the more we can allow human interaction to be focused on higher level, higher risk processes and procedures. That's evolution; that's cognitive security.

### THE FUTURE IS EXCITING

It is our responsibility to ensure we continue with a partner-based strategy. We are more prepared as a community than we will be individually. As we continue to grow, collaborate and sharpen our solutions, we will continue to create synergies, we will shift, and we will grow.

The reality is we can't stop the adversary, and we will never be bulletproof, but the strategy is to make it so difficult and so expensive for the adversary to compromise, that they will move on. Time is money; thus, time is valuable and everything is a moving target.

If we look at the game of basketball — in the most basic explanation the goal is to score more points than the opponent by shooting the ball into the hoop. Now if we changed the target and have the hoop constantly moving in a circular motion, we have increased the complexity and, in essence, changed the game. This is what we, as a technology company, try to constantly do. We are changing the game of print, and we are changing it with increased print security.







Dov Yoran, Sr. Director, Strategy & Business Development Security  
Business Group for Cisco Systems, Inc., talks about big threats, critical moves, ongoing trends and the value of teamwork.

### WHAT ARE THE BIGGEST THREATS FOR ENTERPRISES IN 2018?

The biggest threat is the growing complexity of the enterprise technology landscape. The rapid adoption of IoT devices, with a myriad of security weaknesses, is of particular concern. Cisco's Talos threat research team expects these devices to play a central role in the escalation of attack campaigns against enterprises.

The complexity of the security ecosystem is also growing. Today's enterprises are dealing with numerous security solutions from a multitude of vendors. This complexity creates the potential for unintended gaps in protection and creates inefficiencies in the incident response process. All at a time when skilled security analysts are in critically short supply, and time to detection and remediation is one of the most important measures of security effectiveness.

### WHAT ARE THE MOST CRITICAL MOVES AN ORGANIZATION SHOULD MAKE?

1. Know what your critical assets are and have a plan for protecting them.
2. Security is a team sport. From the Board of Directors on down, everyone has a role in protecting these assets. Make sure each person knows their position and how to play.
3. Understand the security solutions you have in place — their capabilities, limitations and how to use them effectively.

4. At some point you will need outside help. Ensure you have established relationships with your solution vendors. Have agreements in place with incident response firms, before you need them.
5. Always be learning. Regularly evaluate the effectiveness of your defenses and security training programs and adapt as necessary.

### WHAT ELSE SHOULD WE BE FOCUSED ON?

Improving detection and response times. A few ways to accomplish this include simplifying your security infrastructure, interconnecting systems, learning to leverage security data more effectively and employing automation where possible.

### WHAT'S ON THE HORIZON?

Continued regulatory growth, with GDPR in India and Europe for example, and data privacy regulations continue to evolve. Email authentication requirements in the U.S. public sector will spill over into the private sector. And we'll likely continue to see an uplift in ransomware attacks against enterprises and consumers.

IoT-based vulnerabilities are shaping up to enable unprecedented attacks. Cisco threat researchers expect 2018 to be the year of "destruction of service" attacks, for which IoT will certainly play an active role in attempts to debilitate enterprises beyond repair.

On the adversary side, the cyber black market has evolved into a mature and specialized division of labor centered on researching a vulnerability, creating an exploit, servicing that exploit, providing attacks and providing customer services toward that attack — it's an incredible level of sophistication and mature business practices.

### HOW CAN WE BEST PROTECT OUR ENTERPRISES?

Be proactive about security. Make sure everyone knows their role and practice until it is second nature. Encourage an environment of healthy skepticism. Ensure your business partners understand their role and your expectations with regards to your security and theirs.

Collaborate — with industry partners, government, even competitors. Sharing information and knowledge is one of the best ways to stay ahead of adversaries. At Cisco, we have the Security Technology Alliance Program, which helps us to collaborate with other solution providers and ensure that products from different vendors share information and work effectively to detect and manage threats. A great example is the work that Cisco and Xerox are undertaking to help organizations across multiple industries achieve a better state of security.

# The Preventer:

**FAVORITE PHRASE:** Not on my watch.

**SUPER POWER:** Intrusion prevention

**SPECIALTY:** Safeguarding access and data transmission.

He's quick, agile and fearless, delivering the first-in-line prevention that ensures only authorized users have access and can only see what you want them to see.

Adept at intercepting attacks from corrupted files and malicious software, The Preventer prevents any and all attempts at installing infected, non-signed versions. If a file's not legitimate, it's DOA on his watch.

Your office environment  
and vital information  
are safe with us.



SET THE PAGE FREE







# A change in mindset for a shifting landscape

Each new year brings new opportunities and challenges. To help us understand what we should continue to do in 2018 and what and how we should evolve, we spoke to Sergio Caltagirone, Director of Threat Intelligence and Analytics at Dragos. Here is his take:

**“Too many of us are living in the last century of information security. We’re taking the approach that we’re not patching fast enough, not doing asset identification well enough. These things may still play a part in the security puzzle, but the threat landscape has moved well beyond that. Which is why we’re seeing the failures that we’re seeing. We’re still fighting the last war and losing the current battle.**

## **ASSUME YOU’RE GOING TO LOSE.**

We need to approach security with the presumption of loss. We are just now entering that phase of understanding in cyberspace. That’s why cybersecurity insurance has become such a big deal.

Take flood control for example. We have several predictive and detective measures to identify when and how large a flood will be. We have topology maps which identify the locations of critical resources such as hospitals and neighborhoods.

We can prevent normal, everyday flooding. But, in a 100-year flood scenario we triage choosing to protect the hospital over the neighborhood. We need to prioritize detection. We can’t prevent all loss. We need to respond quickly and effectively to our detection. We can’t try to save everything all the time – we diffuse our already extended security resources and no longer focus on the true business risks. We need to change not just what

If we want to move up the security maturity spectrum, we need to shift our thinking from ‘How do I stop the next breach?’ to ‘How do I detect it fast enough that I can do something about it?’

We’re practiced at protecting in depth but to bolster our detection before the full impact is actualized by an adversary, we need to detect in depth as well — which calls for a detection-driven security cycle.

## **THE ADVERSARY IS OUR BEST TEACHER.**

We’ll never be able to know all our vulnerabilities, assets or attack vectors. Adversaries will innovate quicker than defenders. But, that doesn’t mean we’re lost. We own the territory and the infrastructure. Instead of trying to continuously fight last week’s war, we must understand our adversary’s behaviors and ‘control the physics’ of the space.

By that, I mean: Adversaries are going to do many things once they get access to a machine and are able to leverage the associated assets. What are they going to do with the passwords? Can we detect when they’re stored in a file? If not, can we detect when a password is being used, possibly through identity protection? And if they’re assuming identities, can we detect if they’re stealing data? The answer to all those questions is Yes, we can. Rather than thinking of an attack as a single point of failure, but it’s a string of opportunities for the defender to detect and respond. It’s said attackers only need to be right once. To sever that attack thread, defenders only need to be right once, too.

## **SPEAKING OF CLOUD SECURITY PROVIDERS**

The cloud is a critical component of any modern enterprise. Most cloud service infrastructure is more secure than most enterprises – and enterprises need to realize that fact. But, don’t choose your cloud services and security based on a checklist. Security changes so quickly that any checklist is a useless metric. Instead, choose a technology provider that takes security so seriously it’s part of their organizational identity. Only then will you find a partner that moves and evolves quickly in the security landscape not because of a checklist, but because that’s who they are.

## **HOW WE WILL WIN**

Security is not won through procurement, it’s won through people and relationships. Pick the right partners, technology vendors and business partners. That’s how we win with security. Your technological security solutions are your security lower bound. Your people, the defenders, your organization, your relationships that define how great you can be — your upper bound. Make your defenders great, and your cybersecurity will only get better.

## **THE BIGGEST OPPORTUNITY**

We currently have at our fingertips the largest collection of shared computing resources ever in the history of mankind due to cluster and cloud computing. We can collect more data and see more things than we’ve ever been able to before. Our applications are generating telemetry and data more than they ever have and our ability to process it is greater than it’s ever been, and we’re not even tapping this at its full capacity. This is the biggest opportunity — simply taking advantage of this computing revolution that’s right here, right now.”

## **THINGS YOU NEEDN’T WORRY ABOUT.**

With so many things on our minds, especially at the C level, it’s important to know what is not worth spending energy on.

- 1. AI** — As a threat, this is so far in the future that only my grandchildren may have to consider it. We have so many business concerns and modern-day threats to worry about that are here-and-now that AI should not be on anyone’s radar yet.
- 2. Cryptocurrency mining** — That should be something your vendors handle for you at the technology layer. It’s a misuse of your computing resources.
- 3. Cloud breaches** — As organizations move to cloud-based and hybrid-based architectures, we will see breaches within cloud infrastructures. But, given the current state of breaches, it’s hard to say the tradeoff is any worse than where we are today. Most cloud infrastructures are better protected, better managed and more secure than most enterprises.

we’re doing but how we fundamentally think about the problem.

## **PREVENTION IS NOT THE CURE.**

Prevention is critical and always will be, but prevention only gets us so far. We need to reevaluate our current investment to identify where and how we can move to quicker and more effective detection.



We are proud to partner with Xerox, makers of the only print solution with  
the power of McAfee security protection.

Yours. Ours. Theirs.  
All security products working together.



[www.mcafee.com](http://www.mcafee.com)

# The Partner:

**FAVORITE PHRASE:** Let's do this.

**SUPER POWER:** Works well with others

**SPECIALTY:** Recognized worldwide for a comprehensive approach to printer security.

The Partner works with compliance testing organizations and security industry leaders to wrap their overarching standards and know-how around his.

He consistently achieves top levels of compliance with the most stringent certification bodies and can measure performance against the highest international standards.

Your office environment  
and vital information  
are safe with us.



SET THE PAGE FREE



# Rethinking the Security of IoT Systems

By Ersin Uzun & Shantanu Rane, System Sciences Laboratory, PARC, a Xerox company



## ERSIN UZUN

Vice President, Director of System Sciences Laboratory, PARC, a Xerox company



## SHANTANU RANE

Research Area Manager, Cyber-Physical Systems Security, PARC, a Xerox company

IoT systems are collections of networked components — sensors, actuators, controllers, computing devices — that connect the physical and digital worlds.

Much of the world's critical infrastructure, including smart power grids, nuclear power plants, military command centers, smart city installations and transportation systems, as well as emerging applications in smart homes and offices belong to this category. The large industrial control systems have been assembled over many decades, with the goal of achieving a desired set of goals. Power grids, for example, must distribute electrical power across large geographical areas, balancing the supply and demand at various times of the day. To make this possible, the instruments and controllers that make up these systems have been designed to be safe, reliable, easily configurable and interoperable across different manufacturers and standards. Similarly, emerging IoT applications in homes and offices prioritize flexibility and interoperability rather than security and privacy. Thus, securing these systems presents a unique set of challenges.

### SECURITY FOR IOT SYSTEMS NO LONGER AN AFTERTHOUGHT

Until very recently, when designing the architecture of industrial control systems, SCADA (Supervisory Control And Data Acquisition), the architecture used to supervise and manage large industrial control systems was not designed with security in mind. SCADA had evolved in the 1960s from methods that gathered and analyzed telemetry in power systems, with more industrial control applications coming later. From the point of view of network security, it was a simpler time: The ARPANET was just being deployed, and outside of military engagements, attacks on connected infrastructure were not commonplace.

Designers, operators, vendors and users of today's IoT systems no longer have that luxury. These days, attacks on cyber-physical infrastructure are not limited to just data breaches or malware designed to make our computers unusable; they can put human lives at risk. A virus that encrypts your hard drive is a relatively minor inconvenience compared to an attack on a hospital's electrical power supply, or an attack on robotics systems in a manufacturing plant which can endanger the lives of humans.

### WHY IS SECURITY ONLY NOW BECOMING AN IMPORTANT CONSIDERATION?

Over the past decade, we've seen a proliferation of smart devices that possess the capabilities of information processing and network connectivity. The defining characteristic of the Internet of Things (IoT) is that devices, previously restricted to their physical environment, are now connected to a computer network. This network could be a home network, an industrial intranet or even the whole internet. This means that a device, or a gateway that connects a device to the network, is accessible by someone who presents the right credentials, or bypasses the credentials altogether.

As computation and connectivity have become commoditized, they have spawned a plethora of solutions that automate, improve and simplify key tasks in industrial control — from gathering sensor readings on the performance targets of a conveyor-based motor car production line, to verifying the freshness of a food shipment in a smart supply chain, to programming a CNC machine to precisely cut a block of metal into the right shape. They have also, unfortunately, exposed a rich attack surface that can be exploited by malicious hackers.



Consider, for example, the infamous Stuxnet worm that was used to attack Iranian nuclear installations. A malicious program was inserted into the unit that controlled the operation of the centrifuges in the nuclear reactor. This program caused infrequent changes in the speed at which the centrifuges rotate, which, over a period of time, would cause the centrifuges to deteriorate and fail. What made Stuxnet extremely hard to detect was that the telemetry from the centrifuges was spoofed, i.e., whenever the controller was asked to report the speed of the centrifuges, it would still report benign, expected values rather than the altered velocities induced by the worm.

#### **DESIGNED-IN SECURITY IS A WORTHY OBJECTIVE, BUT HARD TO ACHIEVE**

It is often claimed that the way to address this new set of cyber-physical security challenges is to construct systems that are "secure by design." This requires a system designer to develop an understanding of an

attacker's incentives and the various ways in which he or she can compromise the operations of the system. In the recent Mirai botnet attacks, for example, the adversaries accessed their targets using commonly used default passwords, which had never been altered by their users. This simple attack infiltrated tens of thousands of devices.

The goal of designed-in security is to incorporate measures and protocols that will prevent as many known attack scenarios as possible. A bigger challenge for the security engineer is figuring out how to deal with attack methods that are hitherto unknown, and to design the system in such a way that it can mitigate the negative consequences of such novel attacks. This is a precarious undertaking, and for many IoT systems, this type of designed-in security may be hard to achieve. That's because many systems — think of the smart power grid, portions of which may have been in operation for decades — contain legacy equipment with old processes and protocols that must be brought up to date with

current security best practices, a task easier said than done.

#### **IT'S NOT JUST LEGACY DEVICES THAT ARE HARD TO SECURE**

Some industrial and enterprise applications require a new class of lightweight, low-power, cheap sensors that are deployed in swarms of hundreds or thousands. These devices may power up intermittently or be passive and draw power from other devices in their vicinity. They might engage in opportunistic communication with listening devices in their neighborhood, but could remain silent most of the time. The secure communication and storage mechanisms that are typically deployed in cybersecurity solutions are far too complex to be implemented on such lightweight devices. In addition to the conventional protocols for secure communication, secure data storage and key management, we need security approaches that inter-operate across a vast range of device capabilities.

(Continued on next page)



# Rethinking the Security of IoT Systems

(Continued)

## CONNECTION TO THE PHYSICAL WORLD DEMANDS NEW APPROACHES TO RESILIENCE AGAINST ATTACKS

Speaking very broadly, there are two ways in which an adversary can compromise an IoT system. The first way is by infecting a system component or a controller that interacts with that component. Stuxnet was an attack of this type. The second way, much less investigated at the present time, is by directly compromising the physical environment of a sensor or actuator. It is possible, for example, to deceive or “spoof” the readings of a sensor. A research team at the University of Texas recently showed that, by using a powerful enough transmitter, they could spoof the GPS signal being used by a UAV for its navigation. This could force the UAV to follow an unintended trajectory, ultimately leading to its capture or destruction.

As another example, rather than hacking into a temperature sensor, an adversary might surreptitiously discharge a hot or cold gas next to it, causing the temperature sensor to report an erroneous reading to the controller. The controller, not realizing that the temperature reading has been spoofed, may then take unnecessary corrective action. In doing so, it might waste precious energy resources or cause excess wear and tear on its actuators. It might also, unwittingly, take the system into an unsafe state. Cryptographic solutions cannot address such attacks.

### WHERE DO WE GO FROM HERE?

To diagnose attacks caused by resident threats and attacks that originate in

the physical environment, we have to move beyond classical cryptographic approaches and try to understand the behavior of the system we want to protect. If we can construct a mathematical model of the system’s behavior, then a deviation from this model would suggest that an attack is imminent or is being carried out. The operators can then try to isolate the attack, for example, by disconnecting the affected components from the network, or by revoking a set of compromised keys and so on.

How does one construct a mathematical model for a cyber-physical subsystem? A natural way to do this is to gather data from the sensors involved and applying machine learning techniques to derive a model. We can then use anomaly detection to detect deviant behavior that does not conform to the model. Unfortunately, anomaly detection based on machine learning techniques is not always feasible because there isn’t sufficient data to reliably distinguish between normal and abnormal behavior. This strikes us as unusual because we are conditioned to believe that more data will yield more insights; however the situation itself ought not to be surprising: attacks or failures are rare and having usable data to teach those scenarios to a machine learning algorithm are even more rare.

When a purely data-driven approach fails, it might help to model the system not just from sensor data, but from the underlying physics. The magnitude and direction of the current in electrical

circuits, for example, obeys universal laws. Heat diffuses in a material according to a well-specified differential equation. Using measurements of such physical quantities, it is possible to construct “physical” models of IoT systems or its individual components. Comparing the sensor telemetry against such models may provide clues toward detecting and predicting attacks, when approaches based solely on data-centric models no longer suffice. This notion of smart systems being aware of their own model is not new in mother nature; in fact that is how smart and complex organisms evolved to be resilient and adaptive against previously unknown pathogens or recover from unexpected damages to its internal systems.

### IN SUMMARY

While traditional cybersecurity approaches represent a necessary starting point, they will not be sufficient to secure IoT systems of the future. These approaches, which rely on modern cryptography, will help us secure the perimeter of such systems, but they are less helpful if the adversary is already inside the system, or if he or she attacks the physical interface. Therefore, in addition to cryptographers and security analysts, it is necessary to engage with experts working on non-cyber aspects of cyber-physical systems such as physicists, chemical engineers, control theorists and application domain experts. Being successful in creating truly resilient and adaptive IoT systems requires nothing less than a truly interdisciplinary enterprise.

**At PARC, one of our missions is to develop innovative security solutions to prevent attacks on IoT systems and cyber-physical device fleets. To do this, we focus on three research agendas:**

1. Secure-by-design communications platform for IoT systems
2. Secure interactions between humans and cyber-physical systems
3. Security based on hybrid modeling of cyber-physical systems

# No one can afford to ignore information safety, especially when it involves documents.

This threat isn't going away, so take measures to ensure safe practices in all your document infrastructures and processes. When everyone is well informed and on the same page, you can be more confident in your document security decisions.

## Device Factors: What to Know about Securing Endpoints

Your network—the PCs, the servers—need protection, but who thinks about the vulnerability of your multifunction printers? Small and medium-sized businesses create millions of impressions of their data each year using printers and copiers, and much of this information is vulnerable.

**Don't underestimate what's at risk.** The security of your document domain can't be taken for granted, but the networked imaging systems in your organization can become allies instead of risks.



<sup>1</sup>2014 Endpoint Security Survey developed and performed by ESG Research and sponsored by Guidance Software.

## How Vulnerable Are Your Endpoints?

Use this as a guide to discuss security needs and gaps with your team and your partners.



Important Device Security Factors	
<b>Device Vulnerability</b> <input type="checkbox"/> What possible vulnerabilities might expose your devices to attack?	<b>Remediation Assurance</b> <input type="checkbox"/> What happens if a device falls out of compliance with the security policy?
<b>Device Behavior Variability</b> <input type="checkbox"/> How can you ensure devices comply with the policy for network assets? <input type="checkbox"/> What's the enforcement process?	<input type="checkbox"/> Are you alerted when this happens? <input type="checkbox"/> What's needed to bring it back into compliance? Do you have a remediation policy? <input type="checkbox"/> How do you know the policy is in place?
<b>Network Assurance</b> <input type="checkbox"/> Do you have a policy and process for approving device firmware before deployment?	<b>Reporting</b> <input type="checkbox"/> When a network asset comes out of compliance, can you capture data for reporting? <input type="checkbox"/> Is there an audit trail?

To learn more, download our Document and Endpoint Security checklist and discussion guide at <https://www.xerox.com/en-us/managed-print-services/insights/how-to-secure-documents>



# THE EMPLOYEE OF THE MONTH MIGHT NOT BE A PERSON.



## Xerox® ConnectKey® Technology

Introducing a new workplace assistant that goes beyond the expected. An intuitive user interface helps you print from mobile devices, access cloud-based productivity services, translate documents and customize workflows—all with industry-leading security.



SET THE PAGE FREE

[xerox.com/connectkey](http://xerox.com/connectkey)