Cybersecurity Guide:

HACKERS AND DEFENDERS HARNESS DESIGN AND MACHINE LEARNING

TABLE OF CONTENTS
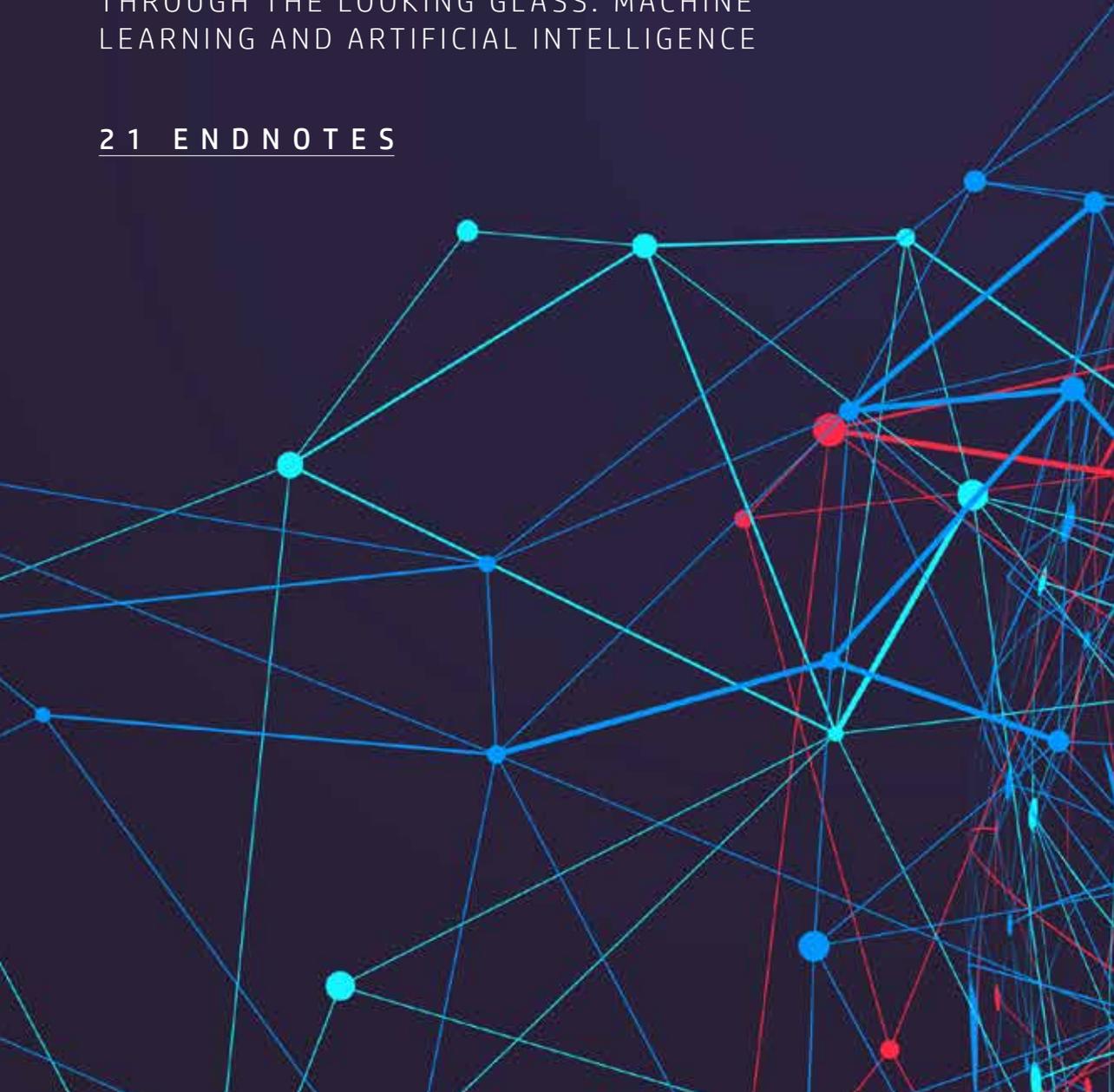
Across the globe, lives and livelihoods are increasingly moving online, physical and digital worlds are beginning to overlap, and digital currencies with no real-world equivalent can buy real-world goods and services. Artificial intelligence is powering autonomous vehicle decision-making,[1] finding new drug candidates[2] daily and personalizing lessons[3] to help students learn. At the same time, doctors are performing life-saving surgeries on the other side of the globe via the internet[4] and robot proxies while networked sensors shake up industries from power generation to public transit. Every year, the list of industries being disrupted by sensors, smart machines, and microprocessors expand.

Just about the only thing that isn't changing is that, where an opportunity presents itself, criminal and political bad actors look to exploit vulnerabilities for gain. And many of the same tools and techniques that are bringing such sweeping benefits to society are also making malicious efforts easier and more damaging. Malware, phishing and distributed denial of service (DDoS) attacks are just a few of the tricks that have piggybacked onto the digital breakthroughs that are advancing our world.

For information-security professionals, successfully defending against the fire hose of now-nonstop online attacks are both the stuff of nightmares and the reason to get out of bed in the morning. Who's winning — the attackers or the defenders?

Given the daily drumbeat of successful intrusions that often cripple companies' operations and erase millions of dollars in stock value,[5] it's hard to tell.

To bring the current and future landscape of cybersecurity into focus, HP conferred with leading experts in the field to create this comprehensive, up-to-date guide. The aim is to help decision-makers who lead information-security efforts at mid-sized and enterprise companies understand all of the options available to prevent damage from cyber insecurity and keep their operations running smoothly.

Section 1:
The situation report

A new malware specimen will emerge on the internet about every four seconds.

Today, 6 million to 11 million new malware infections will be recorded on computers running just one type of antivirus software.[6] Scammers will send over 4 billion phishing emails in the hopes of luring unsuspecting people into clicking a fraudulent link that will let them steal their personal data or gain access to a business network.[7] And a new malware specimen will emerge on the Internet about every four seconds.[8]

An unknown number of hackers will spend about $150 to rent a botnet for a week[9] to launch a distributed denial of service (DDoS) attack aimed at taking down an online service or a network by flooding it with traffic. Cumulatively around the world, these attacks regularly fire 500 gigabits per second of weaponized data at business and government servers to consume network bandwidth and shut the targets down.[10]

Meanwhile, millions of PCs and network-connected printers, cameras, thermostats and other Internet of Things (IoT) devices sit unsecured, with the latest security patches not installed, just waiting for someone with bad intentions to find an open door into an organization's most sensitive data.

The result is a constant stream of news reports about successful intrusions into networks that should be secure. From January to September 2019 alone, 621 ransomware attacks were launched, including incidents that shut down schools and left surgeries on hold as administrators tried to deal with the threats. The costs of these attacks were estimated to be over $186 million.[11] Meanwhile, stories continue to break about vulnerabilities inside microchips that could leave the majority of unpatched modern computers at risk.[12]

It's clear that these attacks — almost all financially motivated — aren't only targeting groups like 2016's Indian bank's data breach[13] or major organizations such as Google, Sony, Equifax, and Yahoo. Hackers are also looking to extort small and mid-sized businesses,[14] health-care providers, municipal governments, and other networks. In fact, there's so much monetary incentive that the threat is mushrooming. One analysis puts the cost of cybercrime by 2021 at $6 trillion — yes, trillion — a value greater than the gains produced by the entire world trade in illegal drugs.[15]

Don't neglect the obvious

These threats are all too familiar to information-security expert Jason O'Keeffe, an HP Print Security Advisor. He knows the bad guys are getting plenty of help from inadvertent computer-user behavior and under-deployed cybersecurity defenses due to many organizations' nonexistent or stretched-too-thin cybersecurity staff.

While assessing companies' computer networks for vulnerabilities, O'Keeffe has seen all kinds of problems that make a hacker's work easier, including glaring omissions by IT departments that should know better.

During one such assessment, O'Keeffe was asked to snoop around a massive manufacturer's IT infrastructure. Among numerous problems, he found that the default factory-set passwords hadn't been changed on 90% of the company's 36,000 printers spread around the network, allowing anyone with the know-how to bypass all security on the devices. Further investigation by O'Keeffe found that many printers were incorrectly configured, which could have allowed an outsider to gain access to the printers and reconfigure them to steal data from the network — or hijack them into service as a botnet. "The VP slammed the table and said, 'Jason, are you kidding me?'" O'Keeffe recalled. "He was fuming."

And with the rapid proliferation of IoT devices and other machines that are connected to both the external-facing internet and a business's internal network without proper authentication required, bad guys have a rapidly increasing array of access points. Gone are the days when an information-security manager could feel the job is done once critical servers at the core of the company's operations are sufficiently protected. Now, that security envelope must extend to the sometimes millions of connected devices in remote offices — and in the pockets of employees.

"We're trying to protect PCs, servers and other core parts of networks, but the IoT devices are the ones that are now putting networks at greater risk," says Shivaun Albright, HP's Chief Technologist for Print Security. "For every 100 lines of source code written, there's typically one defect. So all a hacker has to do is find a defect that gives them entry to the system. We want to make sure we reduce those exposure points as much as possible."

> All a hacker has to do is find a defect that gives them entry to the system.

For every 100 lines of source code written…
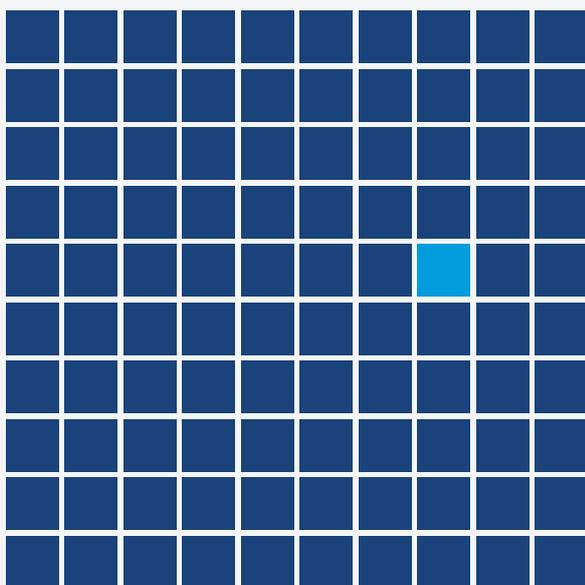
there's typically one defect…

Access everywhere

For today's hackers, the massive profit potential drives innovation and creativity. Among the greatest threats, says Albright, are botnets — the automated tools built out of thousands of hacked IoT devices. To create a botnet, scammers hijack the processors of unsecured machines, then use the compromised devices to mine bitcoin — or they can rent their botnet to others to launch ransom-seeking DDoS attacks.[16]

Given the volume of attempted intrusions happening constantly and the increasing number of ways hackers can get in, O'Keeffe and other experts say it might be better for security managers to think of their perimeter networks as already breached. "What the security community needs to fully accept is that their networks may already be compromised — they just don't know it yet," O'Keeffe says.

Of the 50 plus small-sized and enterprise companies' cybersecurity protocols that he has analyzed, O'Keeffe says every single one of them had vulnerabilities that would allow a hacker to gain access to the network through one of the printers, cameras, mobile devices or other endpoints connected to it.

So the key to keeping a network safe is giving IT workers the tools to detect intrusions and protect endpoints — the easily overlooked opportunities for access that a determined foe will exploit if they're not properly defended. And if there is an intrusion, O'Keeffe stresses, it's critical to have a robust recovery response in place to quickly contain and reverse the damage.

Daniel Kalai, the founder of managed IT service companies that include home and small-business cybersecurity firm Shieldly, agrees with Albright and O'Keeffe that the focus needs to be on securing a network's edges and endpoints.[17] But he believes the pendulum has swung too far from thinking in terms of prevention to an over-weighted focus on recovery. He disagrees with the notion that a compromised network is inevitable in today's digital landscape.

"Cybersecurity used to be about prevention. But now, so much is about remediation. It's a sad way to look at things that comes from people losing faith in prevention tools. But a lot can be done to prevent an attack."

- Daniel Kalai,
  Founder of Shieldly
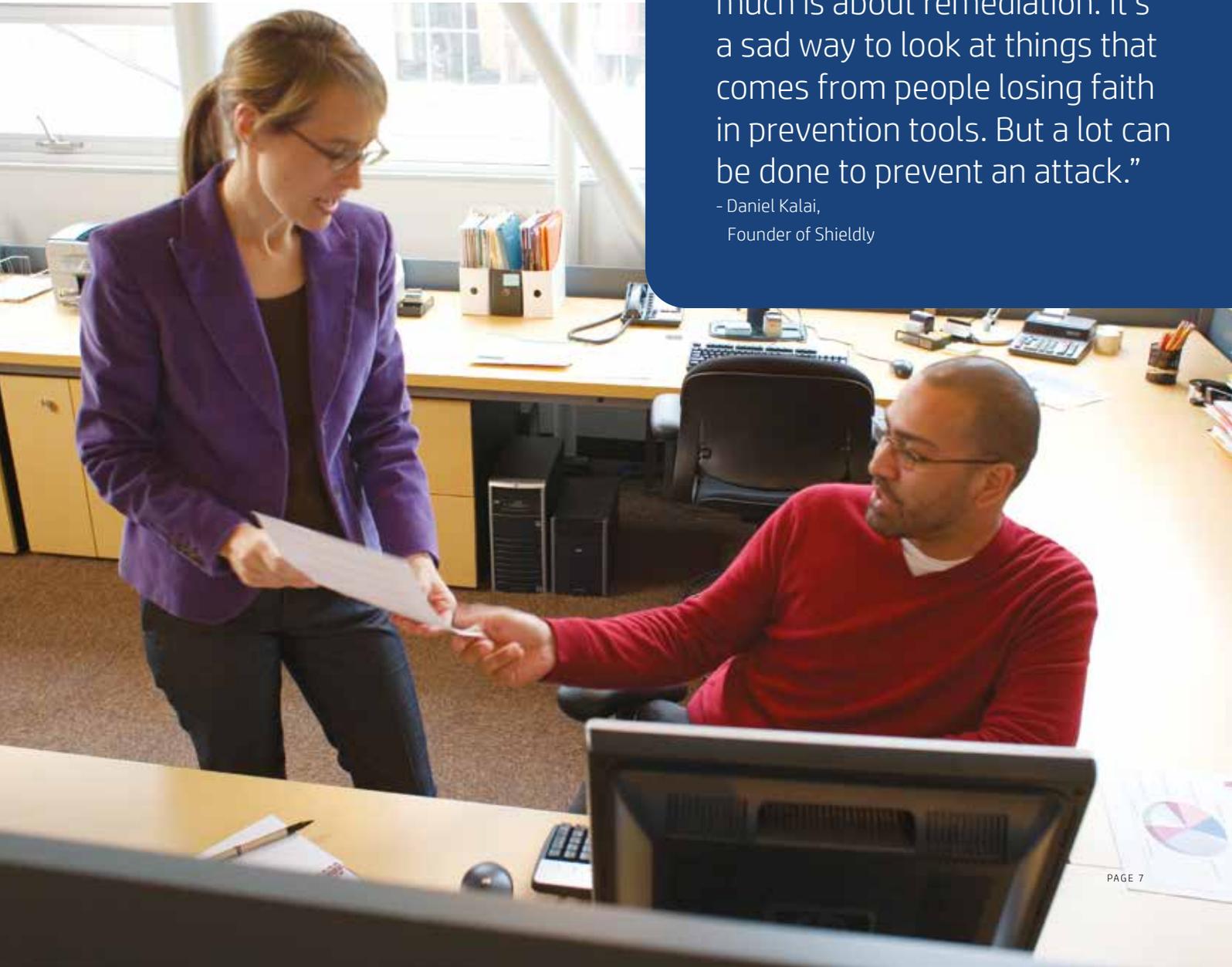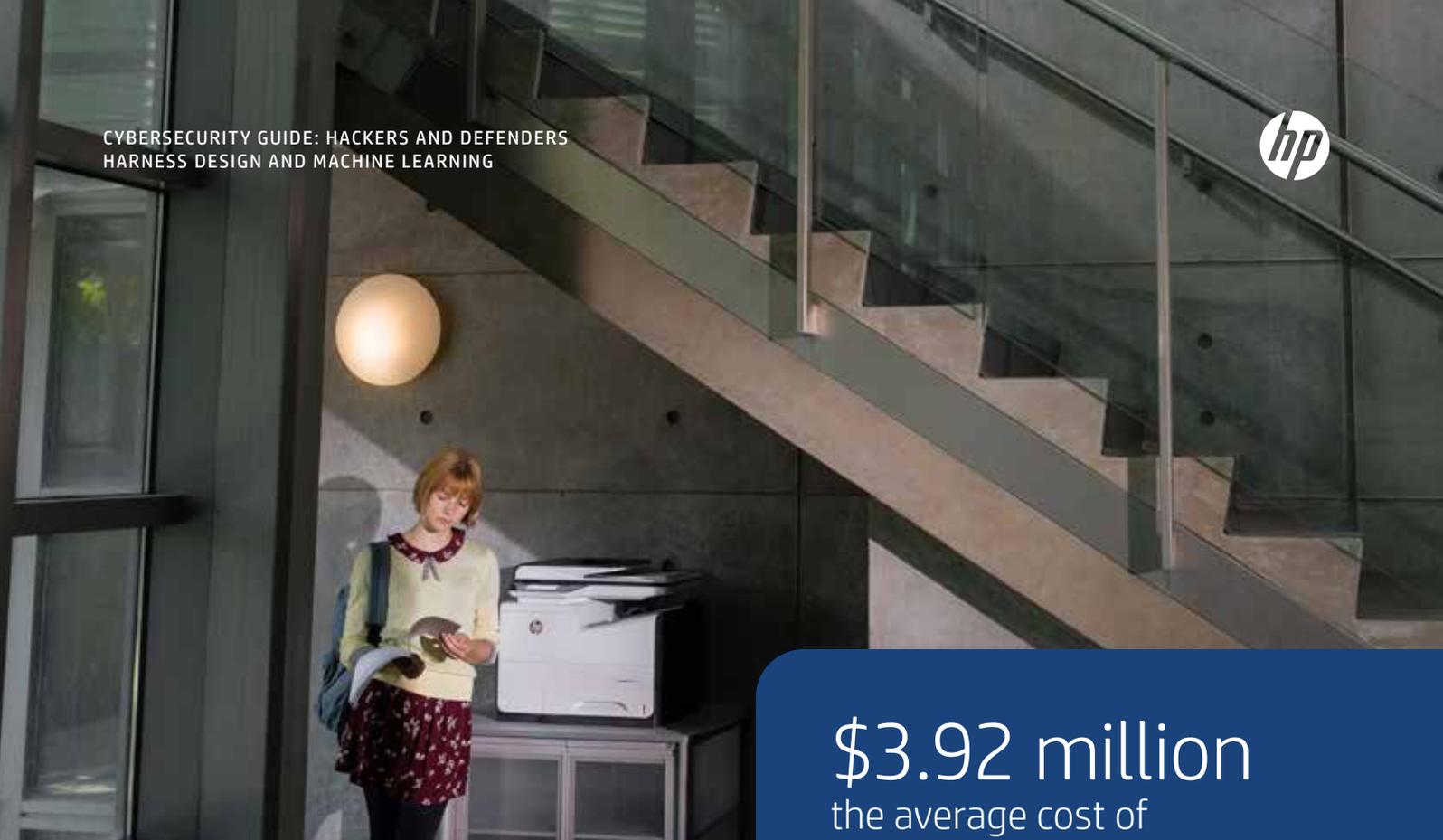
$3.92 million
the average cost of
a data breach
– Ponemon Institute

The price of failure

Better use of security devices, standards and protocols would certainly improve outcomes for those who institute their cyber-defense programs diligently, but real-world numbers show that there's a huge gap between planning and execution. And while the same threats target all organizations, the problem is magnified for smaller businesses because they don't have the same money, time and education resources to invest in security that larger organizations do.[18]

That's why every person charged with a company's information security needs to be reminded of the stakes: the potential for millions of dollars in losses, plummeting credibility and trust in the eyes of customers, lawsuits, and massive business disruption.

According to the latest annual report by the Ponemon Institute, an independent information-security research group, the average data breach costs $3.92 million.[19] Researchers analyzed data breach costs at 507 companies around the world and in 17 industries and found that each lost or stolen record cost an average of $150, a number that quickly adds up with the increasing footprint of these incidents. In fact, the study found that the size of the average breach increased by 1.8% from 2018. It also revealed that smaller organizations had higher costs relative to their size than larger organizations. The total cost for organizations with more than 25,000 employees averaged $204 per employee, compared to $3,533 per employee in organizations with between 500 and 1,000 employees.[20]

Every one of the companies that shared their information with Ponemon reported a breach due to a malicious or criminal attack, a system glitch or human error, with 25,575 being the average number of records compromised in each incident. It took the study's respondents 279 days, on average, to identify and contain the breach.[21]

Malware is getting smarter

Jonathan Griffin, a senior security researcher for HP Labs, says he's seeing more high-profile breaches that deliver a "shocking level of damage and destruction," including 2017's NotPetya, which affected companies in the U.S. and across Europe, and whose primary goal seems to have been purely destructive.[22] As with many other successful attacks, the defense against the now infamous WannaCry was available before the outbreak began. Unfortunately, many organizations, both large and small, had not installed the simple software patches that would have prevented the intrusion.

But successful hacks aren't merely a sign of slipping security. At HP's malware lab, Griffin and his team have noticed that malware has gotten bigger and more complex over recent years. The programs now have considerably better functionality — comparable to a well-designed, high-quality piece of commercial software. Griffin says criminal and state-sponsored hackers are well-organized, highly competent technicians who are constantly improving their craft and incorporating new tools, such as machine learning, which enables systems to learn from experience and improve on their own without being explicitly programmed.

The combination of the growing complexity of attacks and inadequate attention to cybersecurity is amplifying the risks to business networks. Fortunately, Griffin notes, many computer scientists and engineers around the world are working to improve defenses. And experts say organizations are finally realizing that deploying a firewall and antivirus software is just the beginning of an effective program, with layered defenses and intrusion detection essential as well.

Section 2:

Think like Da Vinci: More art is needed in the science of cybersecurity

The term Renaissance Man — for someone whose talents span disparate fields — was created with Leonardo da Vinci in mind. The painter of masterpieces such as The Last Supper and the Mona Lisa was as much an engineer as he was an artist. As a military engineer for almost two decades, da Vinci fortified Milan's defense system while also inventing and improving its weapons. Throughout his life, he also created and refined bridge-building techniques and improved machine components such as worm gears and flywheels. He was an expert in hydraulics and even designed a spring-driven automobile.

The cybersecurity world could take a few lessons from the master. Current and evolving cybersecurity threats demand a blend of art and science — specifically with respect to design.

Those charged with an enterprise's information security must look at all of the physical and digital assets connected to the organization, where they live on the network, how they connect and their relationship to other assets. Perhaps even more important, the real-world use of endpoints such as smartphones, printers and laptops by employees as they do their work should be at the center of security and architecture design.

After all, the best defense keeps the network safe without users even knowing it's there. A useful mantra for information-security managers to keep in mind: Use smart technology, be invisible, and evolve with the threat.

Active monitoring is essential

Allen Kent is a cybersecurity consultant working for NAES Corporation, a company that provides a range of services for industries, from power generation to pulp-and-paper manufacturing.[23] Kent examines power plants up to two dozen times a year looking for cybersecurity gaps and is called into audit power producers, transmission-system owners, and distributors so they're ready for federally mandated checks of their cyber defenses.

> Current and evolving cybersecurity threats demand a blend of art and science.

These federal audits happen every three to six years, depending on how much impact an intrusion into the entity would likely have on the stability of the overall electric grid. Surprisingly, most power generators are usually considered low-impact. The potential for a major impact would arise if there were a systemic problem at the so-called balancing authority control center, which manages fluctuating electricity supply and demand across regions and the nation.

Before he began working with the critical infrastructure of power generation, Kent was in cybersecurity in the banking sector, so he has been figuring out ways to thwart threats from organized criminal syndicates and nation-state entities for years. He says that despite the significantly more work that electric operators need to do to be compliant with federal standards, in contrast with the financial industry, the power sector's cybersecurity is actually OK. "Not great," he says, "but OK."

One of the biggest challenges Kent faces, he says, is educating managers that there is no such thing as a sufficient off-the-shelf cybersecurity solution that they can install and forget. "Defenses need to be monitored constantly," he says. "But most smaller companies in any industry don't want to pay for someone to do that. It's an ongoing expense with no return — until an event happens that dwarfs what that salary would have cost."

Kent tells companies they need to start their cybersecurity program by doing four things: install a firewall and ensure it is properly configured to work correctly; put systems in place that monitor and filter dangerous or suspect content from email and web browsers; separate protected assets from those that don't need the same level of protection (at a power producer, for example, plant-operating computers would be separate from those running business operations); and establish protocols, people and software to actively monitor all of it. This is a standard cybersecurity model called perimeter defense: It builds digital walls and intrusion-detection systems to keep intruders out.

Now, however, there are new weapons available that give cybersecurity managers even more of an offensive game. Not too long ago, experts believed that no prevention strategy could catch every new threat that arises on the internet. But today's automated detection tools are starting to watch their networks in action to learn how data normally moves over them so they can detect and stop intrusions from snowballing into damaging incidents. A seemingly small event, such as a laptop sending several gigabytes of data out of a network that normally transmits hundreds of megabytes, can trigger an alarm.

The four pillars of network cybersecurity:

1 Install a firewall
2 Monitor and filter dangerous or suspect content
3 Separate protected assets
4 Establish protocols

Layers aren't just for winter

"We need to build devices so they have several levels of defense," says HP's Albright. "Defense in depth, we call it. Recognizing that you can't protect against everything, you have to be able to look for and detect anomalous behavior within the device that could be indicative of an attack."

Going a step further, HP Fellow and Chief Technologist Vali Ali says security and detection capabilities need to be built into devices that live on the network, not bolted on afterward.[24] Security intelligence — software that detects threats as they come in, stops them automatically, and purges the machine of malware — has advanced rapidly in recent years. But to work optimally, it must be built in so it's transparent to the user while also being flexible enough to counter a range of attacks.

Also, IT purchases must be made only after careful consideration to find the equipment that will both do the job and protect users and data. "Every device purchase is a security decision," Ali says, adding that security is a combination of technology, awareness, process and governance.

Besides having intelligent detection, response and learning capabilities, networks and devices need to be resilient — to recover in a timely manner after intrusions. "You're going to be attacked," says Ali. "You need to be able to detect, respond, and then recover at speed and at scale."

> "You need to be able to detect, respond and then recover at speed and at scale."
>
> – Vali Ali
>   HP Fellow and Chief Technologist
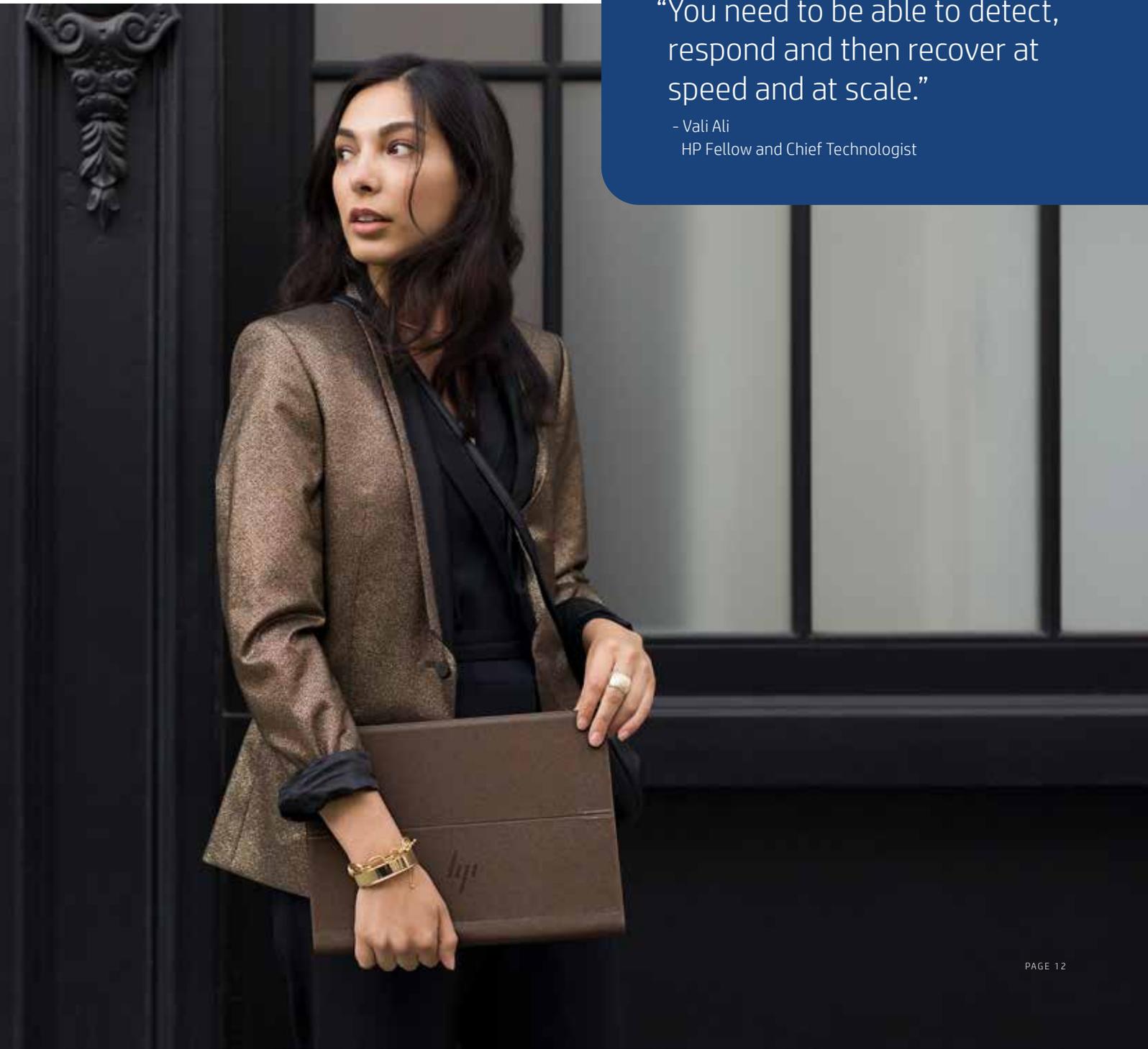
Danger at the network's edge

Some enterprise-scale organizations have the resources to extend protection out to the periphery of their networks. But many mid-sized businesses and enterprises haven't locked down all of their smartphones, scanners, printers, and IoT devices. HP's Albright says her talks with customers often reveal an unexpected lack of concern for securing the endpoints of complex networks.

"What's surprising to me is that a lot of customers are very much aware that their PCs, servers and network devices, such as switches and routers, are at risk, but they typically don't even worry about printers or other IoT devices," she says. "That's where we're trying to drive awareness and education — that any endpoint on your network that has exposure or is not secured can put your entire infrastructure at risk."

But first, IT departments must make sure they cover the basics: 1) develop and adhere to strict security protocols, including requiring that factory-set passwords and maintenance access codes be changed immediately on all devices; 2) maintain timely security-patch and update schedules for all networked devices; and 3) set automatic or urgent updating of operating systems and applications, firewalls and antivirus definitions. Companies must also be diligent about keeping their employee rolls up to date and quickly purge access by individuals who no longer work there.

Ali says it's also critical to incorporate an up-to-date understanding of how the modern office is evolving. Employees increasingly expect to be able to work from anywhere at any time, and work and play often blend or switch locations — work can be done at the beach, while happy hour can take place at work. "Offices of the future have open boundaries," Ali says. "It's a 24/7, 365 kind of environment where your personal life and your work life are mingled up." Network infrastructure, devices, and technologies need to keep up with this shift.

Security researcher Griffin notes that cybersecurity professionals are engaged in an asymmetric war in which they have to be successful every day, but the enemy only needs to be successful once. He offers seven best practices that will boost cybersecurity in the long run:

1 Put in place easy-to-do processes that aren't overly complex or seem like magic.

2 Provide simple, consistent advice to users.

3 Use 2-factor authentication whenever possible since there are so many problems with passwords and business-password policies.

4 Don't buy on price alone. Turn good security policies into good security products into good security-procurement decisions.

5 Don't settle for "security theater" and ticking off boxes when setting your company's security policies. Make sure the security features you're paying for are actually making your organization secure.

6 Produce more meaningful reports by getting analytical tools that show not just how many attacks and viruses your security system stopped in a month but also how many of those were new and unique.

7 IoT device manufacturers should build security into their products from the start and make sure they're "secure by default".

1
Develop and adhere to strict security protocols

… including requiring that factory-set passwords and maintenance access codes be changed immediately on all devices.

2
Maintain timely security-patch and update schedules for all networked devices

3
Set automatic or urgent updating

… of operating systems and applications, firewalls and antivirus definitions.

The importance of employee education

The modern dissolution of office walls exacerbates a problem that has always been central to security lapses — human behavior. Employees skip cumbersome security protocols

in the interest of productivity and are often unaware that some of their online behavior is dangerous. That's why small, inadvertent acts of poor online hygiene are more often than not the source of crashed networks, exfiltrated intellectual property or sensitive customer data and endpoints getting kidnapped by botnets. "There's always someone who will click on a malicious link in an email" says Albright.

One well-known anti-malware company reports that only 3% of the malware they see targets technical flaws. That means 97% of these hackers are using social engineering to get unsuspecting victims to click on a link in a phishing email or reveal sensitive data such as passwords and bank account numbers.

That's why educational initiatives are crucial, both for IT staff, on developing and maintaining strong information-security protocols and procedures, and for non-IT employees, to minimize the sloppy end-user behavior that creates massive security vulnerabilities.

Key points for non-IT employee training include:

- Don't use the same password across different personal and work sites.

- Don't leave sensitive materials on printers.

- Lock your computer and devices when you step away from them.

- Use device screens that prevent others from seeing information on your computer.

- Don't, don't, don't click on links without thinking about it.

How are designers, architects, and engineers of the best systems baking in human behavior to improve how organizations secure their networks and assets?

Future weapons today

Ali and security researcher Griffin point to a number of HP innovations that are now available to the public that doesn't get in the way of user productivity, so workers are less likely to ignore or disable them.

One such advance is HP Secure, a suite of PC-protection tools that includes Sure View, Sure Click, and Sure Start.

HP Sure View[25], an integrated privacy screen for PCs, thwarts others from reading data on users' displays. "That's a lovely security feature," says Griffin. "It's easy to use, users know it's there, and they know what it's doing."

HP Sure Click[26] is a hardware-enforced security measure for web browsers that isolates malware on a virtual machine to keep it from infecting the system. "How many times have you clicked on a link and immediately said, 'Oh, crap, I shouldn't have clicked?'" says Ali. "With Sure Click, malware has no visibility into your actual machine. If malware is accidentally downloaded, users just close the tab and it's gone. It's great because we don't ask users to alter their behavior to make surfing safer."

This kind of user-skipping cybersecurity design will go a long way toward reducing the large human factor in network intrusions.

HP Sure Start[27] rethinks malware defense by analyzing BIOS firmware, the most basic part of a computer's operating system — an area that is increasingly subject to attack because it's very difficult to detect intrusion there. Without a proper defense, malware installed in BIOS is invisible, allowing an attacker to have a persistent presence on the network.

HP Sure Start prevents scammers from living inside a network's BIOS. As a PC boots up, the embedded feature verifies that the BIOS is clean. If it isn't, HP Sure Start restores the code to a clean version automatically, without the user or IT needs to get involved. "This is secure by default," says Ali.
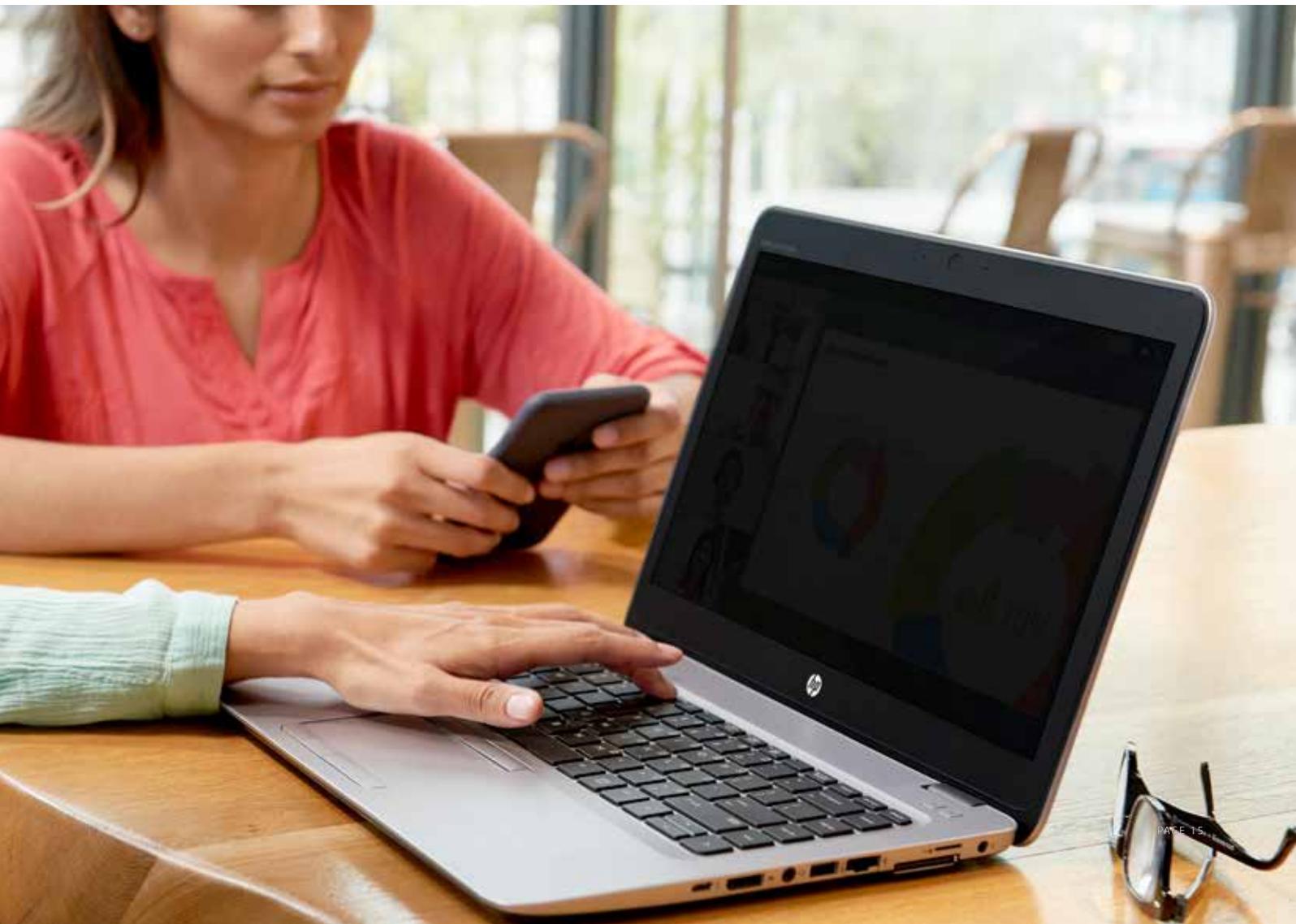
Section 3:

Through the looking glass: Machine learning and artificial intelligence

While the best current cyber-defense practices include layered technology, biometric logins, and network monitoring, combined with good online-hygiene education for employees, keeping our digital neighborhoods safe is starting to get some help from AI via machine learning.

Another HP advance can protect those vulnerable network-connected endpoint printers. Developed at HP Labs and available now, HP Connection Inspector is an intelligent, embedded security feature that learns what a printer's normal network behavior looks like and then watches for suspect changes. When it detects unusual outbound data, it notifies administrators, shuts down the suspect communications, and then forces a self-healing reboot to remove the malware and stop the attack.

These developments are giving NAES' Kent a measure of cautious optimism. He's waiting for the day when technicians can plug a device into the network that watches for threats buried inside data-communications streams, immediately shuts down the data exchange if an intrusion is detected and then studies the details of the attack to deduce what a similar one would look like as it begins. "An artificial intelligence box that monitors everything and stops a threat automatically as it manifests — that would be great," he says.

### Bringing IoT devices under the defense umbrella

Embedding processors and internet access into thermostats, motion sensors, lighting and other systems enable an office building to find significant energy savings on its own based on occupancy, time of day and even the weather. A wind turbine reports back to managers that gears inside its nacelle are vibrating too much and need attention. A commercial jet engine and flight computer work together to make minute changes that decrease fuel burn and shave time off a route.

These smart devices are also coming into our homes in the form of smart thermostats, smart refrigerators, smart lightbulbs and AI-powered digital assistants. In the future, we'll also have smart prosthetics and retinal implants that will be embedded with tiny processors and boast web connectivity. But what happens if hackers target them?

"Think about a retinal implant or an amputee who has a 3D-printed leg, and imagine if that prosthetic gets a firmware attack or is infected with ransomware," says HP's Ali. "What would that look like? What would people do if they suddenly lost their eyesight and got a message saying, 'Please pay up or you can't see'?"

Keeping our digital neighborhoods safe is starting to get some help from AI via machine learning.
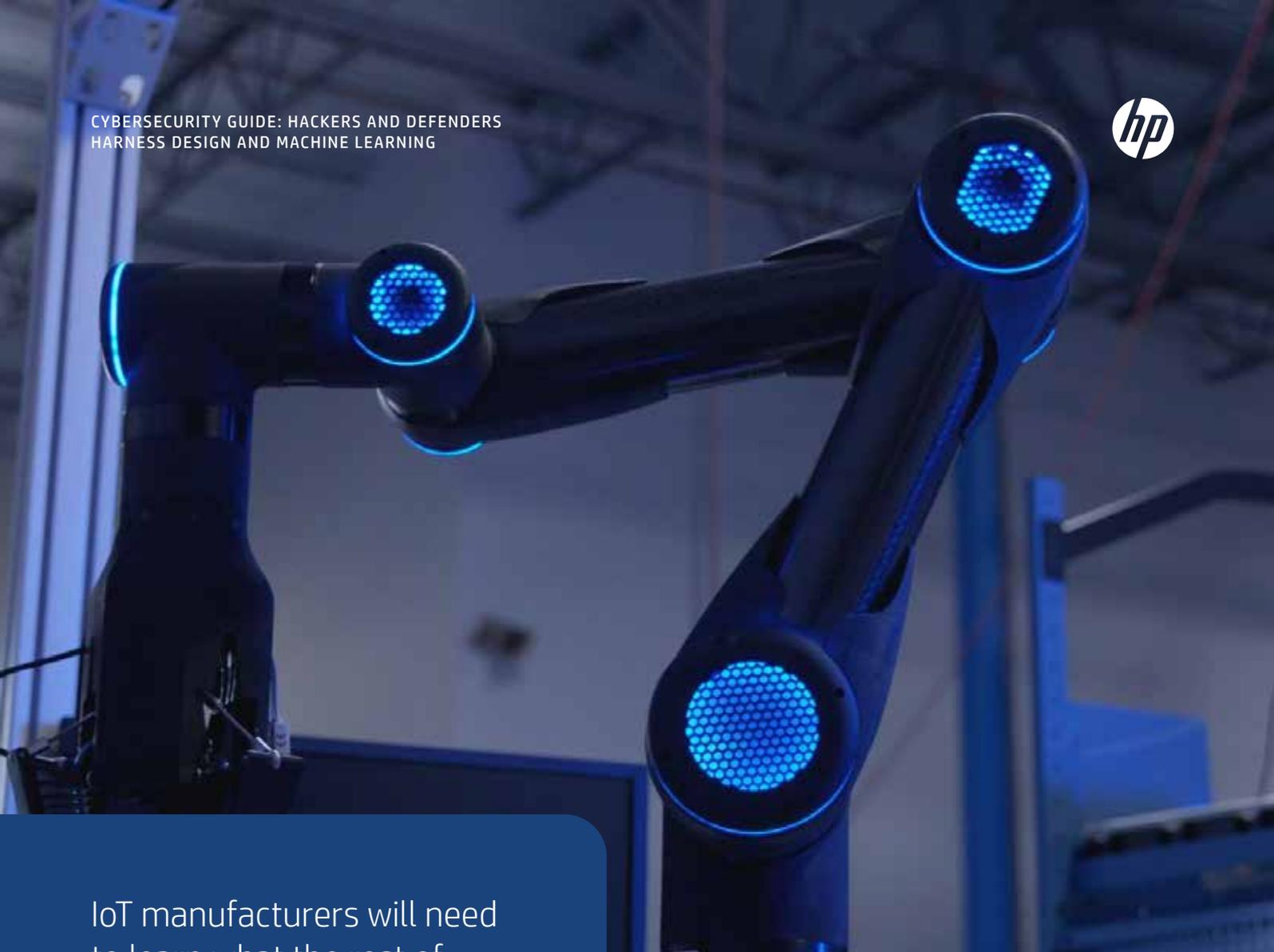
IoT manufacturers will need to learn what the rest of the technology industry has learned over decades of insufficient focus on security: IoT devices need to be built with security at their core.

That's where resiliency comes in, allowing an infected machine to quickly purge the malware and come back online in a clean state. "The moment a retinal implant gets infected with malware or ransomware, all you'd have to do is blink and the malware would go away and vision would be restored," says Ali.

To do this, Griffin says, IoT manufacturers will need to learn what the rest of the technology industry has learned over decades of insufficient focus on security: IoT devices need to be built with security at their core. So if a smart lightbulb gets saddled with malware, it should be able to blink off, reboot, purge the foreign code and blink back on.

Ease of use protects against bad behavior

"If I had to put a key into my door and then wait for an SMS message to verify it was me trying to get into my house, I wouldn't accept that," says Griffin. "It needs to not get in the way so I can get on with my life."

To address this longstanding issue, engineers have been working on login improvements for years, with computer vision-based facial recognition and fingerprint or retinal biometric challenges finally, slowly starting to replace the old alphanumeric passwords.

Another solution, HP's WorkWise technology, which is a free app available on Google Play, creates a secure cryptographic link between an employee's smartphone and computer. With this link, the computer can tell when the user has walked away from it, causing the computer to automatically lock so others won't have access to it. When the user comes back, the computer recognizes them and logs them back in without needing a password. This technology is the definition of getting out of the way by helping users remain secure without asking them to do anything extra.

"There are two types of technology," says Ali. "The kind that people want to use, and the cumbersome kind they have to use. If it's cumbersome security that they're forced to use, they'll eventually find a way to bypass it."

Machine learning is a double-edged sword

The days of malware scanning as the main tool against attackers are limited. Anti-malware software must be updated with known malicious code in order to know what it's looking for. That doesn't help when new malicious code is launched onto the web, which is happening at speeds that are surprising researchers.

On the defenders' side, data plus machine learning are starting to be leveraged for automated network analysis, which crunches data from the constant stream flowing into, out of and across the business network, looking for anomalies. Such computing capabilities will one day watch for spikes in processor activity, for instance, which could signal that a problem is starting. On the attackers' side, of course, machine learning can be used to automate network probing, scanning, and scrubbing.

HP's Griffin says machine learning and other forms of AI are already giving defenders an advantage. But he warns that tools like machine learning aren't a panacea. In fact, machine learning will likely provide a new attack surface for hackers, who are looking for weaknesses in ML-based protections and using ML/AI themselves to design cheaper and more effective attacks. "It's an arms race, and it's always hard to know where attackers will go next," he says.

> "It's an arms race, and it's always hard to know where attackers will go next."
>
> – Jonathan Griffin
>   Senior Security Researcher for HP Labs
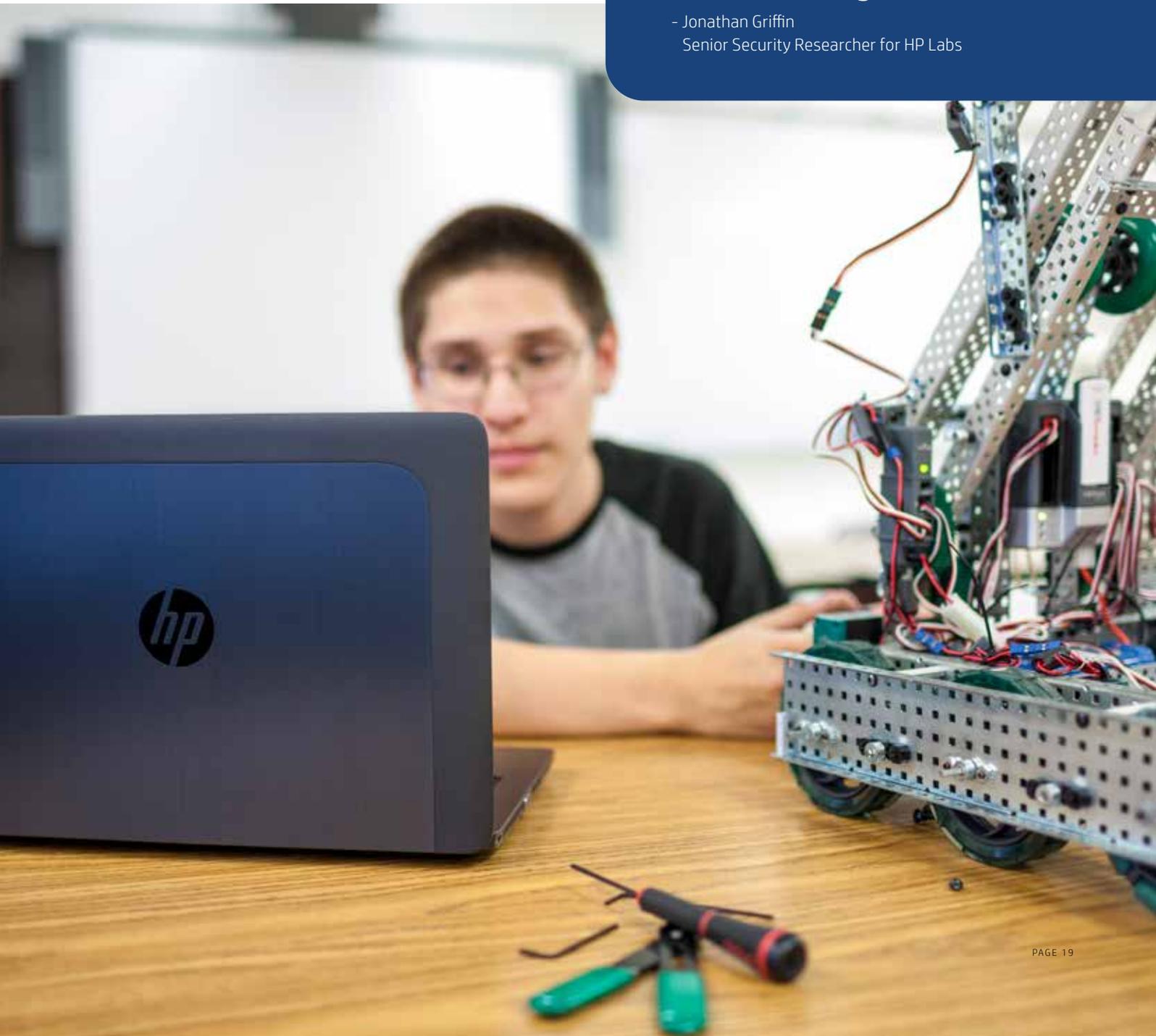
Will AI solve the cybersecurity problem or make it worse?

Further down the road, the advanced algorithms at the heart of machine-learning problem-solving will evolve into more robust AI systems. Attackers with resources behind them will use AI to probe and attack networks. The powerful technology will let them enhance behavioral-engineering tricks to make phishing and malware attacks indistinguishable from legitimate emails and websites. Both attackers and defenders will deploy AI to intelligently reroute network data streams during DDoS attacks to magnify or mitigate the damage.

"We're going to live in a world of AI-enabled smart attacks," says Ali. "It might have already happened, but the system is smart enough that nobody has found out about it."

In the future, engineers should advance AI's dynamic learning abilities sufficiently that defenders' systems will be able to use historical data and current trends to help forecast attacks, thwart or contain them and possibly even hunt down the locations of bad actors.

For now, future-facing manufacturers are just starting to turn the corner on producing devices like the one NAES' Kent dreams of: An AI in a box. The first step is putting security into the heart of products from the beginning of the design process.

Winning the never-ending battle against evil

The cyberwar between the good guys and the bad guys rages on, with uneven outcomes in every industry. With criminal and political elements doing their best to infiltrate and disrupt networks, the stakes are enormous, and the threats can't be wished away.

There's an ongoing fight between the good guys and the bad. It's a fight that we, as good people, cannot lose. It's a fight we must not lose. At HP, we are committed: This is a fight we will not lose.

Protecting the reliability of the digital systems that power critical infrastructure and government, as well as businesses large and small, is fundamental to modern life, livelihoods, and society. "We think it's a scary world out there, but there's good, too," says HP's Ali. "There's an ongoing fight between the good guys and the bad. It's a fight that we, as good people, cannot lose. It's a fight we must not lose. At HP, we are committed: This is a fight we will not lose."

Sources

1 "Self-driving car dilemmas reveal that moral choices are not universal" https://www.nature.com/articles/d41586-018-07135-0

2 "Where Next for AI in Drug Discover," https://www.thechemicalengineer.com/features/where-next-for-ai-in-drug-discovery/

3 "Using AI to personalize education for everyone," https://www.thetechedvocate.org/using-ai-to-personalize-education-for-everyone/

4 "Doctors in China are using 5G internet to do surgery from far away," https://www.newscientist.com/article/2198922-doctors-in-china-are-using-5g-internet-to-do-surgery-from-far-away/

5 "Reports reveals a decrease in stock value after companies suffered a data breach," https://gdpr.report/news/2019/05/16/stock-value-of-companies-drop-7-5-after-data-breaches/

6 Kaspersky, "Cyberthreat Real-Time Map: Local infections in the last week," https://cybermap.kaspersky.com/stats/

7 "One trillion phishing emails sent every year," https://www.techradar.com/news/one-trillion-phishing-emails-sent-every-year

8 "Security Report 2018/2019," https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2018-2019.pdf

9 Digital Attack Map, "What is a DDoS Attack?" https://www.digitalattackmap.com/understanding-ddos/

10 Updated: This DDoS Attack Unleashed the Most Packets Per Second Ever. Here's Why That's Important. https://www.imperva.com/blog/this-ddos-attack-unleashed-the-most-packets-per-second-ever-heres-why-thats-important/

11 "Ransomware's mounting toll: Delayed surgeries and school closures," https://www.cbsnews.com/news/ransomware-attack-621-hospitals-cities-and-schools-hit-so-far-in-2019/

12 "New secret-spilling flaw affects almost every Intel chip since 2011," https://techcrunch.com/2019/05/14/zombieload-flaw-intel-processors/

13 "3.2 million debit cards compromised; SBI, HDFC Bank, ICICI, YES Bank and Axis worst hit," https://economictimes.indiatimes.com/industry/banking/finance/banking/3-2-million-debit-cards-compromised-sbi-hdfc-bank-icici-yes-bank-and-axis-worst-hit/articleshow/54945561.cms

14 "For the Average Hacker, Your Small Business Is an Ideal Target," https://www.entrepreneur.com/article/324711

15 "Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021," https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

16 "Massive Botnet Attack Used More Than 400,000 IoT Devices," https://www.bankinfosecurity.com/massive-botnet-attack-used-more-than-400000-iot-devices-a-12841

17 Telephone interview with Daniel Kalai, Shieldly (January 10, 2018)

18 "Consequences of Poor Security in a Company," https://smallbusiness.chron.com/consequences-poor-security-company-70227.html

19 "2019 Cost of a Data Breach Report," https://www.ibm.com/security/data-breach?cm_mc_uid=21400672026815717196148&cm_mc_sid_50200000=99136091571719614838

20 "Cost of a Data Breach report 2019," https://databreachcalculator.mybluemix.net/?cm_mc_uid=21400672026815717196148&cm_mc_sid_50200000=99136091571719614838&cm_mc_sid_52640000=56277441571719629018

21 https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf

22 Telephone interview with Jonathan Griffin, HP (December 21, 2017)

23 Telephone interview with Allen Kent, NAES (January 15, 2018)

24 "Social Engineering Attacks: Common Techniques & How to Prevent an Attack" https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack

25 HP Sure View integrated privacy screen is an optional feature that must be configured at purchase and is designed to function in landscape orientation. Available on select HP notebooks.

26 HP Sure Click is available on most HP PCs and supports Microsoft® Internet Explorer, Google Chrome, and Chromium™. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files in read-only mode, when Microsoft Office or Adobe Acrobat are installed.

27 HP Sure Start Gen5 is available on select HP PCs with Intel processors. See product specifications for availability.

To learn more, visit www.hp.com/go/explorehpsecure