BRUNSWICK REVIEW

spotlight

on CYBERSECURITY

CODE WORDS
The encryption debate

PREMIUM PLAYER
Cyber insurance comes of age

POLISHED STRATEGY
Avon nails a creative approach

WHERE THE WILD THINGS ARE
Scanning the threat horizon

Plus **BRUNSWICK INSIGHT**
You say privacy, consumers hear security

BRUNSWICK

Brunswick is an advisory firm specializing in critical issues and corporate relations

Spotlight on Cybersecurity is the second in a series that complements the *Brunswick Review*, a journal of communications and corporate relations. Each *Spotlight* focuses on a topic that represents a challenge to corporate leadership around the world. The series launched with a *Spotlight on Shareholder Activism*

To download and share *Brunswick Review* stories go to *www.brunswickgroup.com/review*
Download the iPad app at *www.brunswickgroup.com/review/app*
You can follow us on Twitter *@BrunswickReview*
Highlights from this and previous issues are also available on LinkedIn

EDITOR-IN-CHIEF
Jackie Shorey
jshorey@brunswickgroup.com

DEPUTY EDITOR
Carlton Wilkinson

DESIGNER
Frank Tagariello

ASSOCIATE EDITOR
Edward Stephens

PROJECT MANAGER
Mallory Merge

PRINT PRODUCTION
MerchantCantos

PRINTED BY
CPI Colour

COVER ILLUSTRATION
Noma Bar

INSIDE BACK COVER ILLUSTRATION
Miguel Porlan

FEEDBACK
feedbackreview@brunswickgroup.com

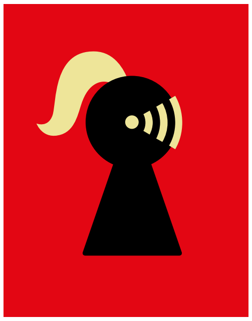
Spotlight on Cybersecurity is printed
on Redeem EW 100% Recycled paper,
made using post-consumer waste
fibers and manufactured without
the use of any secondary bleaching

CAESAR IMAGE: HULTON ARCHIVE, GETTY

1. EXFI, ZXBPXO! (HAIL, CAESAR!)

As long as there has been valuable and sensitive information, people have been trying to steal it. A pictorial series on the following pages takes a look at encryption and security

According to Roman historian Suetonius, Julius Caesar (100–44 BC) protected his military messages by using the "Caesar cipher." Primitive by today's standards, the code relied on shifting letters three places forward or backward in the alphabet. It is likely to have been reasonably secure because many of Caesar's enemies were illiterate.



Cyber threats are generating some scary statistics: $400 billion a year in losses from attacks, with some larger businesses experiencing more than 12,000 attacks each year. But there is also good news. Companies are recognizing that cybersecurity is not a technology concern but rather a critical business issue and one they are preparing to deal with. To address the significant business and reputational risks involved, companies are using a cross-functional, top-to-bottom approach, one that treats cybersecurity as a business imperative.

Many companies are beginning to strengthen their "human firewall," creating a business culture where every employee sees cybersecurity as their responsibility. People, not software, are often the weakest link in a security system and that is a problem no software patch will solve.

Regulation is growing increasingly complex and governments' expectations differ from those of companies and consumers. The rules are murky and lag far behind the technology – and the threat. To deal with competing and at times conflicting requirements, some companies are moving beyond the minimum demanded of them, and aiming for a higher standard.

To be effective, a company's cybersecurity program needs to weave these threads into its underlying business plan. Cybersecurity is more than just a strong defense, more than compliance. It must be a part of corporate culture. It represents an opportunity to differentiate yourself from your competitors, increase the efficiency of your operations and earn a greater level of trust from customers, shareholders and the community.

MARK SEIFERT, GEORGE LITTLE AND SIOBHAN GORMAN
Global Cybersecurity and Privacy practice, Brunswick Group

SOURCES: LLOYD'S, IBM / ILLUSTRATION: NOMA BAR

Decoding the encryption conversation

Brunswick's GEORGE LITTLE and SUSAN HO consider a valuable but contentious tool

Nearly 20 years ago, the "conflicting objectives" of data encryption were identified by the Brookings Institution, a US think tank, as: "civil liberties, economic competitiveness, law enforcement and national security."

These conflicting objectives continue to divide opinion, and encryption is hotly debated by a wide group that includes investors, journalists, governments, business leaders and consumers.

However, encryption's effectiveness as a cybersecurity tool is doubted by none. And a company's approach toward encryption can see them reap huge reputational benefits or, conversely, face reprisals from regulators, the media and consumers.

At its most basic, encryption makes data unintelligible without a "key" of some kind. Digitally encrypted data, for example, may appear as random symbols, letters or numbers. While encryption will not keep attackers from accessing your files it will prevent them from understanding the data. Encrypted hardware means that a lost cell phone or laptop does not necessarily compromise security.

As the distinction between data privacy and data security continues to be blurred, encryption has become almost synonymous with both. (See "Bridging the trust divide," Page 11, for Brunswick Insight's research on this trend.) The mathematics that underpin cryptography are incredibly sophisticated, but to many the encryption equation is fairly simple: it helps keep information secure and private.

Cybersecurity itself is a subject that more and more businesses are prepared to discuss with stakeholders, a conversation in which encryption plays a growing role. Companies that manage this discussion well differentiate themselves from competitors that choose to remain silent. At the same time, those who engage also build trust, communicating to their customers: we care about protecting your data as much as you do.

TECHNOLOGY COMPANIES have been at the forefront of this movement. This makes sense. Tech companies have both the necessary credibility and the incentives. The Information Technology and Innovation Foundation think tank estimates that Edward Snowden's leaks about the US National Security Agency surveillance wound up costing Silicon Valley up to $35 billion in annual revenue, as customers shunned the purchase of new products or equipment that could put their personal information at risk of surveillance.

2. THE KAMA SUTRA (LANGUAGE OF LOVE)

One wouldn't expect to encounter encryption in the Kama Sutra. The ancient instructional guide to the art of lovemaking was put together by Hindu philosopher Vatsyayana, believed to have lived around the 2nd century. One section of the book lists 64 arts that an ideal lover should master. Number 44 is *mlecchita vikalpa*, or "the art of understanding writing in cypher and the writing of words in a peculiar way." Presumably this technique allowed lovers to communicate in secret.

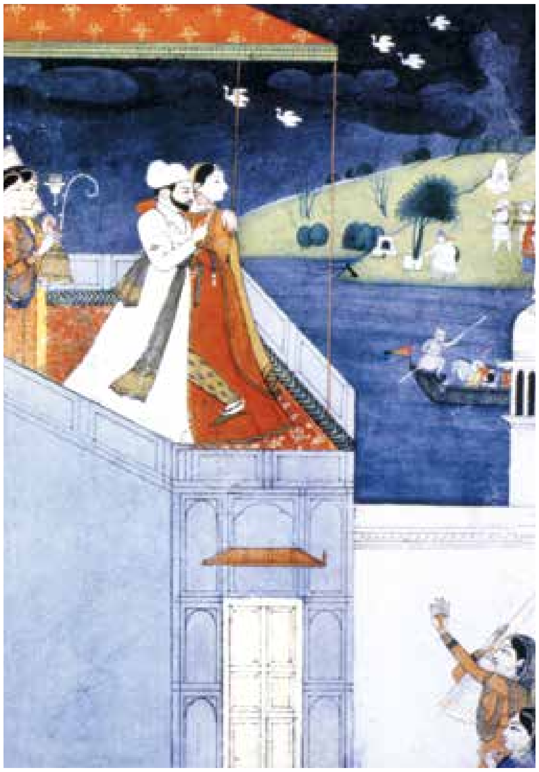


IMAGE: THE GRANGER COLLECTION, NEW YORK

WhatsApp, a mobile messaging application with more than 1 billion users, quietly enacted encryption in 2016. "Privacy and security is in our DNA," it said, "which is why we have end-to-end encryption in the latest versions of our app." The move, "ensures only you and the person you're communicating with can read what is sent, and nobody in between, not even WhatsApp." The feature has been broadly welcomed by users, but it highlights the "conflicting objectives" that the Brookings Institution raised in 1997: some government bodies, increasingly concerned with terrorism and national security, are less enthusiastic (see below).

Telegram, a global messaging application with 100 million users, and Allo, Google's messaging service, have adopted similar encryption measures. The operating systems for both Android phones and iPhones have encryption features built in. Online file hosting services, such as Dropbox, encrypt data stored in the cloud. Microsoft's email service, Outlook, and its suite of Office365 products, are encrypted. All highlight encryption on their respective websites.

THE ENCRYPTION CONVERSATION is by no means restricted to Silicon Valley. Any industry or business that collects and needs to protect data can, and perhaps should, join in.

A 2014 survey conducted by the Pew Research Center found that only 26 percent of American adults trusted that companies with whom they did business would keep their records private and secure. Credit card companies, which scored highest on the survey, inspired confidence in only 38 percent of respondents.

SNAPSHOT GLOBAL SECURITY REGULATION

Even world powers that traditionally reside at opposite ends of the political spectrum tend to be reasonably aligned on the question of data privacy. In general, they want some form of access to encrypted data, citing it as an issue of national security. Many businesses oppose such an idea.

A bill has been introduced in the US that could force companies to decrypt and hand over data, though any progress on the issue is unlikely until after the presidential elections in November 2016. In the UK, the proposed Investigatory Powers Bill contains a similar provision.

Different versions of mandatory key disclosure legislation – as in handing over the key that decodes encrypted data – exist in countries such as Australia, China, France, India, Russia and South Africa.

But global laws on cybersecurity vary widely and extend far beyond data privacy and encryption. Many stipulate disclosure requirements and mandatory cybersecurity measures for businesses.

The EU is set to implement groundbreaking legislation that will come into effect across the continent by 2018. (See "Following the rules is not enough," Page 16, for a closer look at EU regulation.)

Hong Kong's Monetary Authority announced an initiative in May 2016 to improve cybersecurity among banks, the same month that a bulletin was issued by the local regulator to all licensed companies based in Hong Kong with suggestions on how to strengthen their cybersecurity.

In Singapore the Cybersecurity Act, set to be introduced in 2017, will empower the government to play a greater role in managing cyber incidents in the event of an attack on key companies or industries in the private sector.

> "While the regulatory landscape is far from straightforward, compliance alone should not be the goal"

Brazil enacted the Marco Civil da Internet in 2014, described as a civil rights framework for the internet, and this was reinforced by further regulatory legislation in 2016.

No unified legislation on data privacy exists in the Gulf Cooperation Council region, although the alleged 2016 security breach at Qatar National Bank, the largest lender in the Middle East and Africa by assets, has drawn attention to cybersecurity. Some GCC countries are beginning to write laws of their own. Qatar's cabinet approved a data privacy law in January 2016, while Dubai issued a law addressing cybersecurity in late 2015, although specific policies and an oversight authority to enforce them have yet to be implemented.

But while the regulatory landscape is far from straightforward, compliance alone should not be the goal. Companies that take the initiative and set their own standards for data privacy and security will earn trust from their stakeholders that will serve them well in the event of a cyber attack.

This at a time when customers are increasingly reluctant to give businesses either their data or their trust (see "Trust divide," Page 11). Trust is in short supply and businesses are competing with each other to win it. As a 2015 *Harvard Business Review* article said, "In an information economy, access to data is critical, and consumer trust is the key that will unlock it." This is the "data premium," the value an organization gains from effectively communicating its careful stewardship of the precious data with which it is entrusted.

So why isn't every company encrypting every byte of their data? To begin with, encryption costs money and takes time to implement. Often, it also comes at the expense of efficiency, a trade-off not all businesses are willing to make. End-to-end encrypted data can't be easily monetized, shared or studied (See "Safety in numbers," Page 21, on how companies are using their data to tackle social problems). And of course, not all information a company stores warrants such security.

Even if businesses do encrypt their data, they may not be interested in making that practice public. As we have seen, the conflicting objectives highlighted by Brookings remain contested.

In the wake of recent terrorist attacks, law enforcement agencies have said that encryption puts lives at risk by greatly limiting their ability to monitor and investigate dangerous criminals. Others have argued that providing any third-party access to encrypted data is prone to abuse and undermines the security of all information protected by similar encryption techniques.

This debate was inflamed after a terrorist attack at San Bernardino, California at the end of 2015. As part of its ensuing investigation, the FBI asked Apple to unlock an iPhone that belonged to Syed Farook, one of the alleged perpetrators. Apple offered to assist the FBI in other ways but didn't create a code to unlock the phone, saying that doing so would jeopardize the security of all iPhones and set a dangerous legal precedent. The FBI eventually accessed the phone without Apple's help, but both sides agree that the broader issues raised by the case remain unsettled.

3. AL-KINDI (PATTERN RECOGNITION)

الجمهورية العربية السورية
SYRIA
THE 6TH CONFERENCE OF THE ARAB MINISTERS OF CULTURE
بريد
1987
POSTAGE
البيروني
330

The 9th century Iraqi polymath Abu Yusuf Ya'qub ibn Ishaq Al-Kindi, commonly known as Al-Kindi, pioneered frequency analysis, a powerful codebreaking technique. Certain letters and spelling constructions occur more often than others. A symbol that appears most often in a coded message is likely to correspond to the letter most commonly used in that language's alphabet, and so on. Frequency analysis went on to be used to crack codes in many languages for centuries afterwards. Syria is one of many countries to release a postage stamp honoring Al-Kindi (left).

THE PERCEPTIONS surrounding encryption, about what governments need to do – and should be able to do – in the name of national security, vary widely by culture and by country. This can make encryption a sensitive and complicated topic for businesses with a global presence to navigate.

Striking a balance in both tone and message is difficult, but critical. Businesses that broadcast the strength of their encryption could motivate an attacker to try to prove otherwise or, in certain countries, face a backlash, and perhaps legislation. Those that describe their "AES 256-bit-encrypted" hardware will be understood only by the most tech savvy, while companies that oversimplify the issue may have their competence called into question.

In such a delicate environment, businesses may be wary of saying anything at all. Talking about encryption can be contentious. But the bigger risk is to leave customers in the dark about what is being done to protect their data.

GEORGE LITTLE is a Partner in Brunswick's Washington, DC office, specializing in crisis, cybersecurity, reputational and public affairs. **SUSAN HO** is Head of Brunswick's Hong Kong office. She was formerly Global Head of Brand at Standard Chartered. Additional reporting by **SIOBHAN XIAOHUI ZHENG,** a Director in Hong Kong who specializes in cybersecurity.

Precious ore, precious data

A digital future opens an old industry to new threats, says Brunswick's CAROLE CABLE

No one knows exactly what the mine of the future will look like, but we can be sure of one thing: it will be a target for hackers. Mining may not seem an obvious place to find cybersecurity risks, but the industry is transforming fast. Commodity prices have fallen 52 percent since 2011 and mining productivity is down 3.5 percent per year over the last 10 years, according to a 2015 McKinsey report. In response, the industry has turned to digital and technological innovation to help preserve cash in the short term, and capture value over the long term.

Mining operations are often in remote locations, with variations in geology, metallurgy and weather extremes. New technology is helping mitigate such variability by lowering risk and cost while increasing safety and productivity. "We believe this to be the future of mining," says Pedro Fuenzalida, Innovation Manager at Antofagasta Minerals. Analytics can "deliver a step change in productivity," he says.

Digital tools already move equipment fleets and driverless trains, schedule maintenance and manage the global supply chain. Drones and scanning equipment create 3-D maps of underground areas, and robots are being developed to mine hard-to-reach resources. Rio Tinto's fleet of autonomous trucks has driven the equivalent of 98 times around the earth to deliver loads 24 hours a day.

"Our operations are increasingly digitized," says Richard Williams, COO of Barrick Gold Corporation. But this progress has a downside. "Data flows from one point to another, which makes it open to attack," he says.

In 2012, Saudi Aramco revealed a cyber assault on its systems, to "stop the flow of oil and gas to local and international markets," Abdallah al-Saadan, Aramco's Senior Vice-President of Finance, Strategy and Development, said at the time. While it didn't succeed, damage was still done.

In 2015, Canadian company Detour Gold was hacked, putting at risk credit card numbers and employees' personal data. And in 2016, Canada's Goldcorp had 14.8 gigabytes of sensitive data accessed and posted on a public website by "hacktivists," with a message railing against "corporate racism, sexism and greed."

Meanwhile, the industry has been poor at disclosure and communication of how it assesses, manages and mitigates cyber risk. Of the top 20 global mining companies, just 12 mention cybersecurity as a risk in their 2015 annual reports. Among them, disclosure varies widely: from a minimal statement saying the topic was discussed by the Audit and Risk Committee, to a vague outline of the potential impact of attacks. Only one classified a potential breach as a "reputational risk."

As the mining industry depends more on digital technology, stakeholders will look for a balance between transparency and secrecy, creating value and protecting it. This is not an IT issue. Everyone in the company must take responsibility. "People see risk as a separate subject managed by specialists," Williams says. "But cyber risk being managed by IT is the same as leadership being managed by HR – it feels like a function and is not owned at the highest level of the organization."

CAROLE CABLE is a Partner in Brunswick's London office and co-leads the Global Energy and Resources practice.

NO BUSINESS IS IMMUNE

Anyone with data can be a target, says Brunswick's Will Rasmussen

Consider this scenario: a hack into the interconnected systems controlling major office buildings causes chaos by triggering fire sprinklers, creating sauna-like temperatures and manipulating critical equipment. "It's not something that real estate investors really had to think about before, but it's definitely on our radar screens now," says Tom Murray, a Principal Partner at New Mill Capital, a real estate investment firm.

No business that stores or transmits information is immune from cyber attack. Some sectors have so far avoided data breach headlines, but threats and risks continue to increase.

Antony P. Kim, Global Co-Chair of the Cybersecurity and Data Privacy team at the law firm Orrick, says the number of businesses boosting preparations has increased sharply. "No organization is too boring or unattractive to a hacker," Kim says.

Sectors with little history of attacks are often at greater risk. Recent reported hacks in the computer systems of cars, and even a jet's in-flight entertainment system, shook the transportation sector. In 2016, hackers manipulated a US water treatment plant. A year earlier, a German steel mill reported massive damage after an attack disabled blast furnace controls. Surprising targets include small businesses and nonprofits.

"Ask these questions," Kim says. "Do we use computers? Do we use the internet? Do we create or handle data? If your answer to these questions is yes, then you are a viable target for the bad guys."

Unclear but present danger

Brunswick's MARK SEIFERT and SIOBHAN GORMAN explain that the breach you dread may come from an unexpected source

Security technology company McAfee has reported that its "malware zoo" – where it logs all the malicious software, or malware, it discovers – has grown at last count to 433 million species, around 70 percent more than the previous year. While it is hard to forecast what cyber attacks and cybersecurity will look like a decade from now, it is a safe bet that McAfee's zoo will continue to welcome millions of new, and increasingly nasty, predators each year.

Yet 44 percent of organizations polled by software company CyberArk in 2015 believed they could keep cyber attackers off their networks entirely. In an environment where new threats emerge, evolve and proliferate at increasing speed, this level of confidence is alarming – and reckless.

Cyber threats pose a risk not just to security, but also to reputation. A strategy to address these risks has to acknowledge the likelihood that company defenses will be penetrated, and it should include plans for a response when the attackers gain access to company systems.

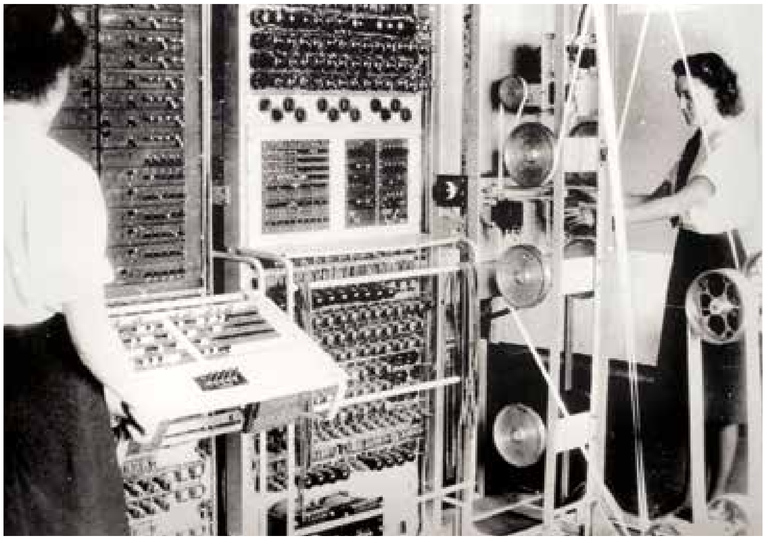
One of the fastest-growing forms of attack globally is "ransomware," where a hacker locks a user out of their data until a ransom is paid. McAfee reported more than 4 million types of ransomware in 2015, 1.2 million of which were new. "Never before in the history of humankind have people across the world been subjected to extortion on a massive scale as they are today," said Symantec, a software security company, in a report on ransomware.

The total cost of these attacks extends well beyond the ransoms paid, says Keith Jarvis, a senior researcher at SecureWorks, a global information security company. Jarvis says the bill "likely extends into the hundreds of millions of dollars annually," after factoring in business disruption and lost data. Each of the most prolific types of ransomware can be responsible for millions of spam emails, Jarvis says. At one time, individuals were most at risk. Now the targets are large and corporate: hospitals, law enforcement agencies, energy companies and even school districts.

Whether in search of publicity or as a tactic to apply pressure, ransomware attackers may tweet their demands. Once out in the open, companies will face questions from investors, employees, customers and law enforcement. Those who are unprepared may have to scramble to formulate answers and coordinate a response while locked out of their emails and internal networks.

Ransomware can become especially complicated in jurisdictions such as the US, where it is illegal

4. COLOSSUS (CODE BREAKER)



Colossus was the name given to computers built by the British during World War II to decode the Lorenz cipher, a code used by senior German officers that was even more complicated than Enigma, which Alan Turing had helped solve. Lorenz was first compromised by human error (see "The heart rules the head," Page 14). Colossus went on to analyze and decipher massive volumes of coded messages. Designed by Thomas H. Flowers, who was influenced by Turing's work, Colossus is considered the first large-scale electronic computer – before that, machines had been solely electro-mechanical. Pictured above, Royal Naval personnel operate a Colossus computer in 1943 in Bletchley Park, British code breaker HQ.

PHOTOGRAPH: BLETCHLEY PARK TRUST, GETTY

to pay money to any person or organization on a terrorist watch list. While such demands are often linked to organized crime, some terror groups may use ransomware to finance their activities. If the attack succeeds, and a company chooses to pay, it should work with specialists and law enforcement to avoid legal or reputational fallout. In addition to technology-based defenses, companies can also educate employees to avoid "phishing" attacks, the most common vehicle for this kind of malware.

ATTACKS THAT MANIPULATE or compromise data are another growing threat. James Clapper, US Director of National Intelligence, says data manipulation will soon become the most dangerous form of cyber attack facing businesses. "Decision making by senior government officials, corporate executives, investors or others will be impaired if they cannot trust the information they are receiving," he told the US Congress in 2015.

Manipulated data poses significant risks both to individual businesses and to the broader marketplace. If your data can't be trusted, how will customers be able to trust you? What decisions will you be able to make with confidence? Perhaps most frightening of all: what happens if you don't even know that your data has been changed?

Attackers unable to breach your defenses may instead focus on your business partners. Target's highly publicized breach in 2013, when roughly 110 million customer records were compromised, began with an attack on a third-party vendor.

The following year, Benjamin Lawsky, one of New York State's senior financial regulators, sent a letter to dozens of banks requesting information about third-party service providers. "It is abundantly clear that, in many respects, a firm's level of cybersecurity is only as good as the cybersecurity of its vendors," Lawsky wrote. The data agrees with him. In its 2015 Global State of Information Security Survey, PwC found breaches attributed to business partners climbed 22 percent.

Vendors performing mundane functions can often be found to have unexpected and worryingly high levels of access to a company's network. Imagine explaining to your customers why you allowed a copy machine vendor access to their data. Companies should consider cybersecurity when selecting business partners and regularly review those they already work with. What third parties have access to your networks, and under what conditions?

> **"Imagine explaining to your customers why you allowed a copy machine vendor access to their data"**

Many companies store data and run business-critical operations and applications via the cloud. This is cost-effective, efficient, and can provide a more secure system than many businesses can create on their own. But, as is true for all modern technology, the cloud is not immune to attack.

A hacker need only piggyback on one of the hundreds – or thousands – of businesses using the cloud to attempt to gain access. Once inside the cloud, the hacker can then launch a distributed denial of service attack, overwhelming the system by flooding it with requests from within and crippling the operations of all the cloud service provider's users. The fallout could be disastrous for any business and create a legal and communications minefield.

At this point, things can get very complicated. Some companies might wish to keep the matter quiet; others may prefer to go public. Meanwhile, an investigation by the cloud service provider could raise further questions of privacy, since it might need access to a company's data in order to determine the extent and nature of the attack.

Affected companies might be tempted to blame the cloud-hosting service, but doing so runs the risk of appearing to shirk responsibility. Suing the cloud provider is an option, but that might fuel further public attention and controversy.

COMPANIES CANNOT IMMUNIZE themselves from these threats. However, the damage can be mitigated if some precautions are taken: have a crisis response in place for each scenario, run cyber attack simulations, educate and train employees, analyze and tackle your vendors' vulnerabilities, and bolster cybersecurity measures. Even simple steps, such as stronger authorizations for data access, can help, and should be a part of a regular review of cybersecurity practices.

Instituting best practice well in advance puts a company on a firm footing should it need to explain or defend its actions in public. "We did all we could," is always a much stronger response than, "We didn't see it coming."

MARK SEIFERT is a Partner in Brunswick's Washington, DC office and co-leads the firm's Cybersecurity and Privacy practice. **SIOBHAN GORMAN** is a Director in Washington, DC and advises on public affairs and crisis, with a focus on cybersecurity and privacy.

BRUNSWICK INSIGHT

Bridging the trust divide

Consumers see little difference between data privacy and security, says Brunswick Insight's PETER ZYSK

Your company might have a cybersecurity officer and a privacy officer, with separate responsibilities. The problem is, your customers don't think that way.

New research from Brunswick Insight finds that consumers around the world rarely distinguish between data privacy and data security. While data is becoming increasingly important to companies, consumers are expressing a growing fear of data theft and a deepening skepticism about how their personal information is collected and protected.

As a result, they are beginning to withhold information, exhibiting newfound caution. A US Department of Commerce study found that privacy and security concerns stopped nearly half (45 percent) of US households on occasion from some online action such as shopping, banking or social activities.

Our survey of more than 7,000 consumers across Asia, Europe and the Americas shows that clear communication about data protection policies can go a long way toward easing consumers' security concerns. Consumers know that their personal data is constantly being collected and they recognize that their online privacy may be diminished as a result. In the survey, the most frequently used term selected to describe company data collection practices is "intrusive."

This response is not just simple irritation, but downright fear – so much fear, in fact, that in many countries concerns about the security and privacy of personal data top those about the economy, war, healthcare or climate change. Consumers are three times more likely to be afraid of how companies may use their data than excited about the potential for innovation and advancement. Companies clearly need to do more to communicate the benefits of data collection.

As a group, organizations that collect data receive little benefit of the doubt. Nearly two-thirds of consumers (62 percent) believe companies should do more to protect personal information, and nearly half (43 percent) say they trust companies with their data less than a year ago. This finding is consistent worldwide.

> **"Remember: when you say "privacy," consumers hear "security"**"

The research also shows consumers consider a company's privacy policy in the context of their security concerns, heedless of the distinction companies draw between privacy and security. Companies may claim to use only "aggregate" or "anonymous" data, but those terms fall on deaf ears, failing to specifically address customers' concerns about data theft.

There are three things companies can do to better meet consumer expectations:

Use a cross-functional team To create an integrated data narrative, you need to involve wide representation from across the company.

Keep security front and center Your safeguards are a critical part of your message. And remember: when you say "privacy," consumers hear "security."

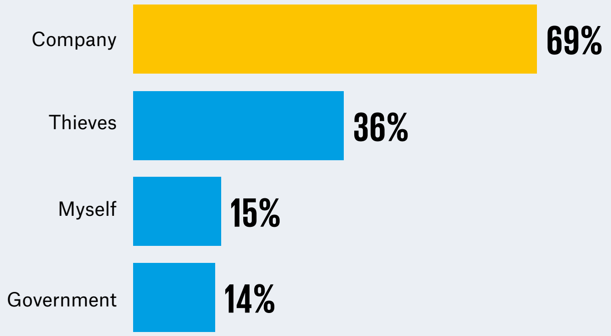
Prepare When bad things happen in the cyber realm, companies have to assume they will be blamed. Prepare now, to reduce the potential reputational harm.

PETER ZYSK is an Associate in Brunswick Insight's opinion research practice and is currently based in Beijing.

ACCOUNTABILITY

IN A BREACH, WHO WOULD YOU BLAME?

Who would you blame if a business you use was hacked, and your personal information stolen?



Percentages do not total 100, due to multiple response options

◀ **Consumers hold companies to a high standard when it comes to protecting their personal data. Even if a hacker were responsible for the loss of consumer data, consumers would blame the company. In addition, most consumers said they would stop buying from the company and encourage others to do the same (see "Ready to boycott," Page 13)**

Data security and privacy top the list of consumer concerns in five out of seven countries surveyed. Exceptions include the US, where the economy is the top worry, and Germany, where the chief fear is terrorism

RANKING THREATS

HOW CONCERNED ARE YOU ABOUT…

Security of my personal data	Privacy of my personal data	State of the economy	Terrorism or war	Access to healthcare	Climate change	Security of my job
87%	86%	80%	76%	74%	73%	58%

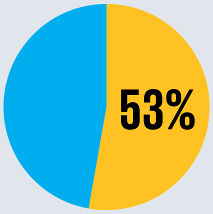
Data combines those that selected “very concerned” and “somewhat concerned”

Corporations can do a better job of explaining how they protect personal information. It seems clear that when companies say “data privacy,” consumers hear “data security.” A majority of consumers in our survey selected a security-centric definition of data privacy

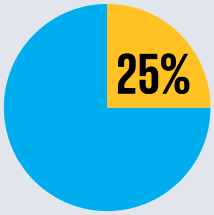
DEFINITION OF TERMS

PRIVACY AND SECURITY ARE BLURRED

How do you define data privacy?



Collected data will not be used or accessed by **unauthorized individuals or parties**



Collected data will only be used for **agreed purposes**

Participants were asked to select the description that best describes data privacy. The two shown here ranked highest

In a separate question about data privacy concerns (how companies use the data they collect), the theft of personal information was the overriding concern of more than 64 percent of respondents – double the number worried about the improper sharing of information

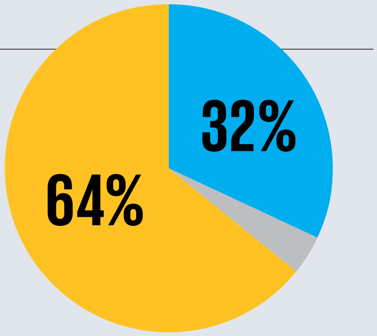
SECURITY IS THE TOP CONCERN

What is your main data privacy concern?

🟨 I am most concerned about my personal information being **stolen by hackers** or compromised in any other way that could make me a victim of identity theft

🟦 I am most concerned about companies recording my physical location or online activity and then **selling or sharing** this information with other companies

⬜ Unsure



BRUNSWICK INSIGHT

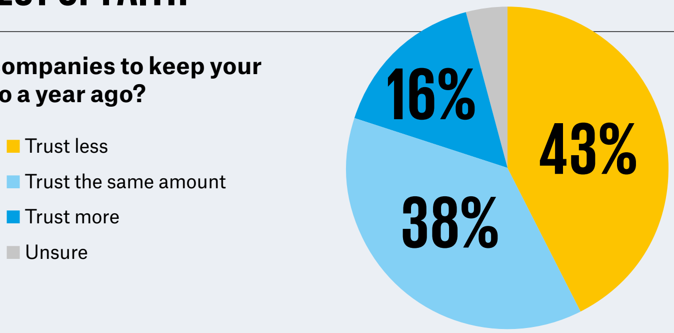
Brunswick Insight provides critical issues research for market-moving decisions, and combines experienced, data-driven counsel with an emphasis on rapid research and analysis. Insight converts research into strategic advice for communications programs and campaigns

This research is based on a February 2016 Brunswick Insight survey of 7,029 consumers in Brazil, China, France, Germany, Singapore, the United Kingdom and the United States. A nationally representative sample of around 1,000 consumers was surveyed in each country

TRUST

BREACHES ARE A TEST OF FAITH

How much do you trust companies to keep your data secure, compared to a year ago?

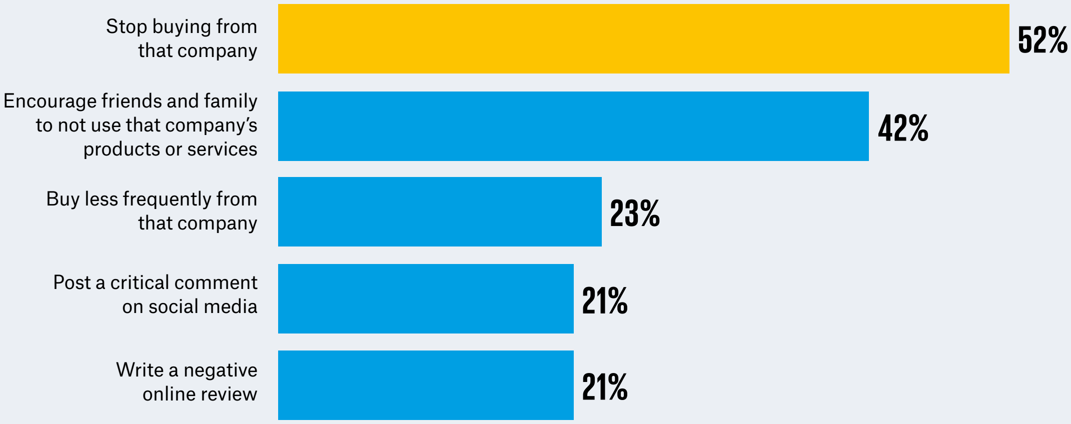


As incidents of computer hacking grow more frequent, consumers' trust in companies is declining. According to the Breach Level Index by business security company Gemalto, the number of hacking events rose globally 9 percent from 2014 to 2015

BOTTOM-LINE IMPACT

READY TO BOYCOTT A BUSINESS

What would you do in response to a breach?



Percentages do not total 100, due to multiple response options

In a clear indication of the reputational and financial risk from a data breach, more than half (52 percent) of consumers globally said they would stop buying from a company in the event of a breach. Nearly half (42 percent) said they would encourage others to join them. Consumers in France (60 percent), Brazil (58 percent) and Singapore (56 percent) appear the most likely to boycott a company

PREVENTION

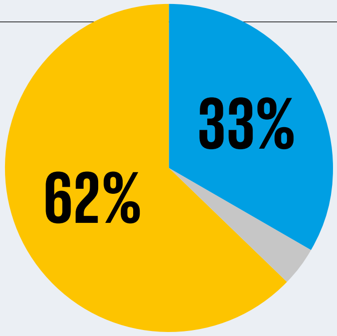
EXPECTATION OF MORE PROTECTION

Are companies doing enough to prevent data breaches?

🟨 Companies **are not doing enough** to prevent data breaches and need to take significant actions to improve the security of their storage systems

🟦 Companies **are doing enough** to prevent data breaches, but the rise in usage of debit cards, credit cards and online payment systems, as well as increased capabilities of online thieves, means that data breaches are just the "new normal"

⬜ Unsure



Aware that advances in digital technology are fueling the rise in breaches, consumers still feel companies should do more to improve the security of their personal information. Each of the first four months of 2016 saw an increase in records lost or stolen in data breaches, according to Gemalto

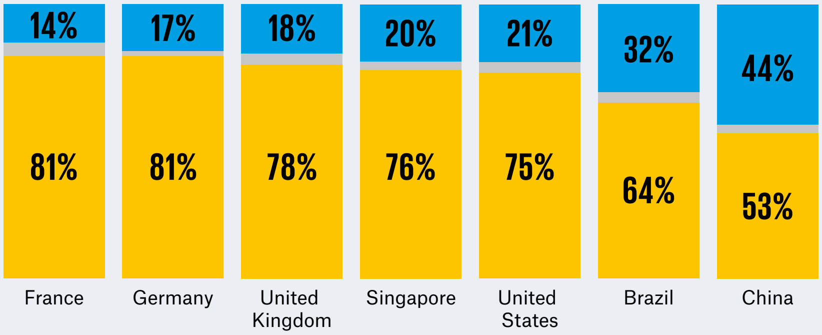
FEAR FACTOR

COMPANIES NEED TO COMMUNICATE BENEFITS

How do you feel about how companies are using personal data?

🟨 I am **scared** by how companies use my data. Data breaches are happening more frequently as hackers and criminals become more skilled at getting through security systems and firewalls

🟦 I am **excited** about how companies use my data. More data allows for more innovation and technological advancement, and greater personalization of experiences



The proportion of responders that said they are unsure, indicated in gray, ranges between 2 and 5 percent

◀ **Communicating the positive role of data in a company's business can promote customer loyalty. However, getting past consumers' strong emotions around the security of their data can be a challenge. Survey responses use words such as "intrusive," "private" and "caution" to describe data collection practices. Turning that perception around requires a dedicated effort and clear messages**

The heart rules the head

Good decisions need good feelings, says Brunswick's ROB ALEXANDER

We like to see ourselves as rational, sensible beings who make considered, data-led decisions, and when we describe a decision as emotional it is usually a synonym for poor or foolish. But how often have you decided to have "just one more glass," a muffin rather than an apple or taken the elevator rather than stairs? Our decision making is less rational than we like to think and often moves us to choose a less sensible path, or even one that may not be good for us.

This kind of behavior has a direct bearing on discussions about cybersecurity. People are the critical component of any company's data protection plan. How they feel about the company and its data policy colors how they behave.

Neurologist Antonio Damasio, in his 1994 book *Descartes' Error*, shows that people actually need emotions in order to make choices. The book features a case where the part of the brain that enables emotions was damaged; the patient had strong cognitive function and IQ scores but was almost totally unable to make decisions.

Yet it is obvious that emotions can lead to bad decisions. The code breakers at Bletchley Park during World War II cracked the highly complex Lorenz cipher as a result of a rash decision by an irritated German teleprinter operator. When a recipient requested a long, 4,000-character message be re-sent, the annoyed sender took shortcuts, using the same settings and, even worse, abbreviations to make his task easier. That breach of protocol was enough to allow the code to be broken. Armed with this key, the allies were eventually able to read Hitler's personal messages to his high command. (See "Colossus," Page 9.)

> **"Our decision making is less rational than we like to think and often moves us to choose a less sensible path"**

Emotions have also been shown to affect how we respond to the advice and input of others. In a study published by researchers at Harvard and Wharton in 2008, the accuracy of answers given by subjects varied dramatically according to their emotional state. Angry emotions led to accuracy being reduced by more than 30 percent and made subjects more inclined to disregard advice.

With a topic as sensitive as the use of personal data, or as detailed as a company data security policy, it is critical for a company to take into account this non-reasoning aspect of decision making. The best way to ensure a constructive response is to provide a positive emotional context.

ROB ALEXANDER is a Partner in Brunswick's London office. After 20 years as a strategic planner in advertising, he leads the Campaign Planning team.

Beyond walls

A strong defense is only part of the story, say PwC's DAVID BURG and MEGAN HAAS

A cybersecurity plan should look much the same no matter where you are. After all, the risks for companies are largely the same everywhere in the world.

However, there are some distinctions to be found between regions, notably in Asia. Here, the insider threat can be more serious than elsewhere. In some Asian countries, there is a history of loyalty to family-led companies, but mentorship and other ways to build employee engagement and empowerment are still a small – if growing – part of the business culture. Where loyalty is strong, insider leaks of information are likely to be less common.

Systems and infrastructure haven't kept pace with the explosive front-office growth that we have seen in Asia, leaving security holes that can be exploited. For multinationals, this outdated technology can hamper the execution of an effective global cybersecurity policy. When companies have grown through acquisitions, they may have 15 different kinds of platforms around the world. A standardized system in all offices is essential for consistency in expectations and reporting.

As elsewhere, appointing the right people to boards to handle issues around cybersecurity can be a challenge. There is a global shortage of board members with the necessary expertise and experience, making constructive policy changes, or dealing with a crisis, harder.

Corporate leaders in Asia can be reluctant to share information about breaches which could help other companies be better prepared. Regulations in the region generally don't require disclosure of an incursion, and there is a cultural element – family-dominated enterprises that might want to avoid embarrassment – that inhibits a freer sharing of data breach information.

Still, public disclosures are on the rise. The Hong Kong Monetary Authority is working with the financial services sector to make information regarding incidents available. And we're hearing from Hong Kong-based CIOs that company representatives are cooperating among themselves less formally.

> “Stakeholders value a company more highly if it is able to push past the fear, uncertainty and doubt, to develop a more constructive approach”

For multinationals operating in Asia, it is important to have a global cybersecurity policy that can then be implemented locally. Tailoring must be done for each region, but realistic minimum security requirements and guidelines on the company's appetite for risk need to be established that apply across the whole firm. Any organization that has a strictly vertical approach on a country-by-country basis is really going to be missing important risks.

In general, companies around the world are moving beyond a strictly defensive posture and starting to see cybersecurity as an asset and a part of a larger strategy that involves the whole business. More are realizing that security by design, at the inception of a product or service, can be a differentiator in the market – a strategic enabler.

In 2015, the World Economic Forum's survey of Fortune 500 CEOs found that cybersecurity was regarded as one of the biggest challenges their companies faced. In at least three Asian economies – Japan, Singapore and Malaysia – a cyber attack was ranked the No. 1 risk for businesses.

In this climate, it has become increasingly clear that stakeholders value a company more highly if it is able to push past the fear, uncertainty and doubt, to develop a more constructive approach. Yet in the minds of too many board members cyber still equals IT. Data security is seen as something very technical, handled by tech folks in the back office.

A global trend among corporations, and even some regulators, is to demand that cyber be a separate component – a peer of IT, reporting directly to the CEO and the board. Currently, data protection is most often under the purview of the chief information officer – strong evidence that it is still viewed as an IT issue. The creation of a new position, a chief information security officer for example, is a really important shift, helping raise the stakes and spread responsibility for data resources throughout the company.

As these challenges are addressed and cybersecurity is integrated into a larger strategy, companies are better able to reap the rewards of collected data used wisely and securely, building trust and creating value.

DAVID BURG and MEGAN HAAS

David Burg is a Principal in PwC's US Advisory practice based in Virginia. He is the firm's Global and US Cybersecurity Leader. Megan Haas is a Partner at PwC in the firm's Forensic Services team and is based in Hong Kong. Operating in 157 countries, PwC is one of the world's largest professional services firms and one of the top four auditors.

David Burg and Megan Haas spoke to **JAMAAL MOBLEY**, an Associate in Brunswick's Washington, DC office and part of the Cybersecurity and Privacy practice.

Following the rules is not enough

The EU is reshaping the regulatory landscape, but smart companies will do more, say Brunswick's PETER LINDELL and ANNALISA BARBAGALLO

In 1995, a tiny company called Cadabra, deciding its name sounded too much like "cadaver," settled on a new one: Amazon. It sold books online and filled orders out of a garage. That was the same year the European Union adopted the Data Protection Directive that regulated personal data privacy.

While Amazon went from garage-based startup to a market capitalization of more than $300 billion, the directive was not as successful. Its principles were interpreted and enforced differently across the EU, and they were also challenged by profound changes in technology and the explosive global development of companies such as Amazon.

5. THE FLOPPY DISK (DATA GOES PORTABLE)

First sold in 1971, the floppy disk transformed data sharing. The earliest floppies were a cumbersome 8x8 inches, but suddenly data was portable, accessible – and easy to steal. Smaller sizes followed. Most were replaced by CDs and, later, USB flash drives – but not all. A report by the US Government Accountability Office recently revealed that the Department of Defense was still using 8-inch floppy disks to "coordinate the operational functions of the United States' nuclear forces." This veteran technology is scheduled to be retired by the end of 2017.

PHOTOGRAPH: MIKE LEDRAY, SHUTTERSTOCK

Two new pieces of legislation, the General Data Protection Regulation (GDPR) and the Network and Information Security Directive (NIS Directive), are poised to modernize and standardize Europe's laws on data privacy and cybersecurity. Their reach could even extend beyond European borders, and potentially apply to companies outside Europe whose customers include EU citizens.

These laws will affect the way companies collect and protect consumer data, and change the extent to which European governments can regulate – and punish – businesses. Companies breaking these rules will face fines as costly as 4 percent of their global revenue or €20 million ($22 million), whichever is greater.

While the new regulations are significant for their scope and severity, they point in a direction where many companies are already headed. As these organizations have realized, there is no need to wait for regulations to create robust cybersecurity policies or to be transparent with customers about how their data is being used and protected.

THE FIRST PIECE OF LEGISLATION, the GDPR, is set to become law across the EU in 2018. When it does, it will give EU citizens greater control and visibility of their data held by third parties.

Consumers will have to give consent for companies to collect their data and this consent must be tied to a specific service or product. Clear wording will be required; no more lengthy, indecipherable agreements.

The GDPR will also require that within 72 hours of a data breach that could jeopardize "the rights and freedoms" of its customers, companies will be required to inform both regulators and those whose data may have been compromised.

Customers will also have a "right to be forgotten," allowing them to ask companies to delete data. This aspect of the law has already been applied in some individual cases and supported by a ruling of the European Court of Justice.

THE SECOND piece of legislation, the NIS Directive, has not yet been passed by the European Parliament but is expected to be approved. This directive places stricter security requirements on all companies based in the EU, and mandates that companies in critical sectors, such as energy, finance and healthcare, inform government regulators of significant disruptions and breaches. In what some have seen as a controversial move, the list of critical sectors has been expanded to include technology companies such as Cisco, Google and Amazon.

While these laws are both expected to come into force in two years, it remains to be seen how they will be interpreted and enforced, and the extent to which they will be challenged in court.

However, four things are clear. First, companies must be fluent in the new regulations and ensure compliance. Armed with popular support and public funding, it is safe to assume regulators will actively police and enforce the new laws. Consumers and the media are also tuned in and, along with regulators, will be asking new questions. Breaches are likely to be expensive and highly visible, especially given the new disclosure requirements. The reputational cost will almost certainly be greater than any direct fines.

Second, given their importance, these regulations should not be thought of as solely an IT issue, a compliance issue, or even just a public affairs issue, though the new laws will have repercussions on all three. In the C-suite and boardroom, this is a business-critical issue that leaders should be thinking about and planning for. What steps are in place to ensure employees are learning about and complying with the latest regulations? Who will communicate with regulators? What does it mean for your business if regulators bring formal charges?

Third, training is paramount. Every employee with access to the company's network poses a risk against which even the most advanced security system cannot guard. Creating a healthy company culture is the best route to security and compliance, and that requires more than handing out copies of the latest regulations. (See "Nailing security," Page 24, for an example of a creative approach.)

Finally, while technology and the regulatory landscape have changed, the principles of good business have not. That means considering the needs of all stakeholders. Companies able to collect and monetize data have a distinct competitive advantage. The more credible a company is at explaining the purpose and benefit of the data it collects, the greater this advantage can be.

A strategy to avoid fines and escape punishment is not enough. Instead, companies need to find ways to use cybersecurity and data collection to separate themselves from the competition.

> "While technology and the regulatory landscape have changed, the principles of good business have not"

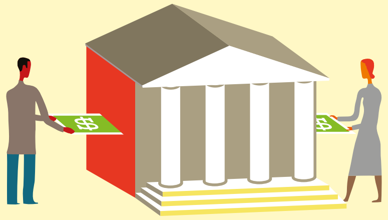
PETER LINDELL is a Partner in Brunswick's Stockholm office and part of the Cybersecurity and Privacy practice. He also advises on M&A, crisis and corporate communications. **ANNALISA BARBAGALLO** is a Partner in Brunswick's Brussels office and advises in the digital and financial services sectors.

6. TYPEWRITERS (PULLING THE PLUG)

Some have suggested that the best way to make a computer secure is to unplug it. In the wake of embarrassing and even dangerous leaks, some governments have explored that strategy. In 2012, Russia's Federal Protective Service, a government body tasked with security, spent 486,540 rubles ($15,000) buying 20 typewriters to help prevent leaks of important documents. In a 2014 interview, a member of the German government said it was considering similar measures. As fans of Cold War spy novels can attest, typewriters do not prevent data being stolen, but filing cabinets full of papers can't be compromised with a single mouse click.

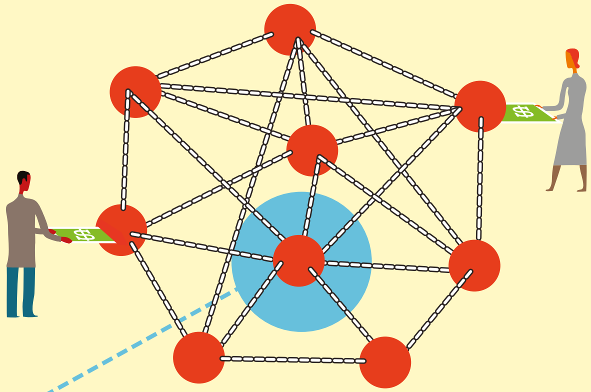
IMAGE: RÜSTEM GÜRLER, GETTY

Blockchain explained

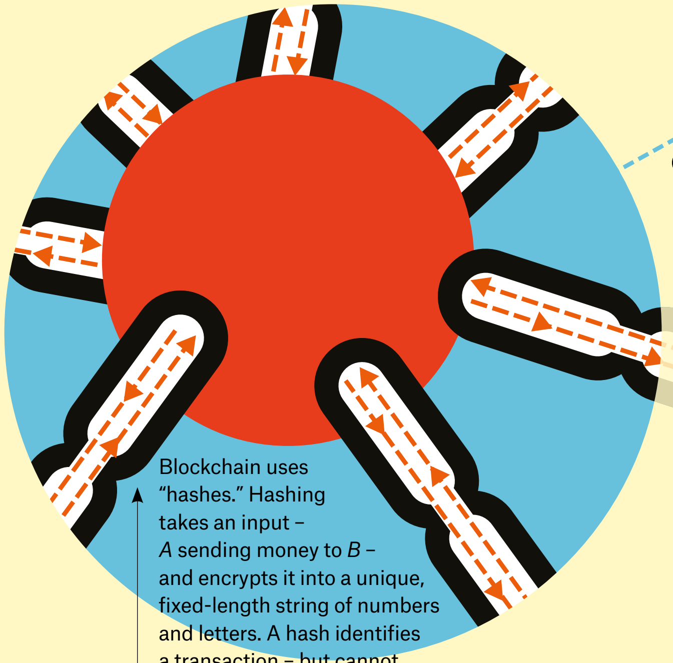


1 Most transactions rely on third parties. To transfer money, a bank processes the request, makes the payment and updates account information. The system is centralized – everything goes through the bank – and requires high levels of trust in the institution handling the transaction

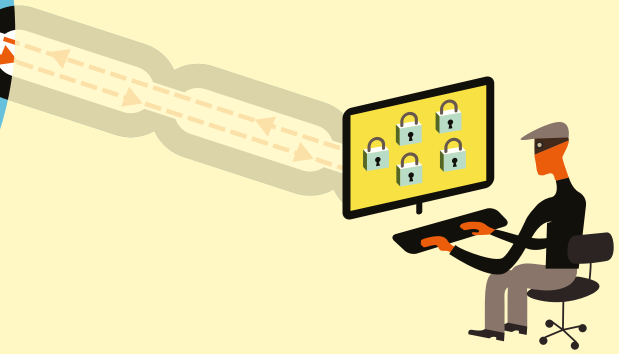
2 Transactions on a blockchain are decentralized. Each transfer is encrypted and distributed across the entire blockchain network of "nodes." Every node has a copy of the encrypted data. However, the information cannot be deciphered, changed, hidden or deleted through any node



3 Blockchain is what its name suggests. When a transaction, or a block of data, is transmitted, it is then verified by a majority of nodes within the network through a process called "consensus by distributed cooperation." Once verified, that block of data is added to the chain



Blockchain uses "hashes." Hashing takes an input – *A* sending money to *B* – and encrypts it into a unique, fixed-length string of numbers and letters. A hash identifies a transaction – but cannot be used to compromise it



4 Blockchain uses layers of encryption to verify and protect transactions across its huge network, making it much harder to attack than a single database. Even if one node is hacked, the blockchain updates continually as new transactions take place. Each new block contains code from the one before, locking the transaction in time, so a hacker could not alter data without alerting the entire network

From *Vice* to the *Financial Times*, blockchain – the "distributed ledger" technology that underpins the digital currency bitcoin – is being talked about as the future of cybersecurity. One of its defining features, that it is decentralized, is what makes blockchain so safe and potentially transformational.

Used mostly for financial transactions, blockchain could be applied to any task that keeps records. Votes could be tallied or company shares stored and traded on a blockchain network. Personal identities and land titles could also be treated as blocks of data to be recorded, protected and verified.

"The notion of shared public ledgers may not sound revolutionary or sexy. Neither did double-entry book-keeping," said *The Economist* in 2015.

Blockchain's transparency is considered one of its greatest strengths – a feature not often associated with security. Take political elections, for example. With blockchain, every voter would be able to track their vote and check that it had been awarded to the correct candidate. Each vote would have to be verified by a majority of the network, greatly reducing the risk of it being excluded or counted twice. And even though the ballots cast would be visible to everyone on the network, encryption would ensure they remained anonymous.

There is, of course, no guarantee that blockchain is perfectly secure. But at a time when trust in public and private institutions is waning, blockchain challenges the idea that you need to trust those with whom you do business. Blockchain is so secure and transparent, some believe, you can simply trust the system instead.

WRITTEN AND RESEARCHED BY EDWARD STEPHENS, BRUNSWICK NEW YORK / ILLUSTRATIONS: OTTO STEININGER

LEGAL PERSPECTIVE

Taking aim at a moving target

Cyber lawyer RAJESH DE tells Brunswick's SIOBHAN GORMAN about lessons learned during his time with US intelligence

Rajesh De was General Counsel for the US National Security Agency during the period when Edward Snowden, a government contractor, copied secret documents detailing the NSA's surveillance practices and leaked them to the international media. The breach had severe repercussions not only for national security but also for governments and companies all over the world, exposing a threat that all data-collecting organizations face.

Now a Partner with international law firm Mayer Brown, De heads its Cybersecurity and Data Privacy practice, advising on the legal and reputational aspects of data risk. Cybersecurity is not static, he says, but "a moving target," and organizations need a long-term commitment involving every aspect of their business.

How did you end up focusing on cybersecurity?
I served in the White House as the Staff Secretary for President Obama, managing the documents that go across the President's desk. I handled all sorts of threat information – increasingly related to cyber. That was when cybersecurity became my passion. Later, as General Counsel at the NSA, I had a pretty good view of the types of cyber attacks the commercial sector was seeing.

What were the biggest cyber threats you encountered during your time at the NSA?
We saw an evolution of attacks, including some that really woke up the public to the cyber threat, such as those on Wall Street and at Sony Entertainment. It taught me how much public trust depends on secure networks.

What are the biggest lessons for business from the Edward Snowden breach?
Preparation, preparation, preparation. The NSA is prepared for many things, but we were not sufficiently prepared for managing this sort of significant leak by an insider. Dealing with the legal, reputational and public relations consequences all at the same time was not something that the agency – which prides itself on its secrecy – was prepared for.

Public opinion can be shaped very quickly, and it takes a long time to undo those perceptions. After Snowden's leaks, stories that had misstated or included incorrect information were almost impossible to fix. Those are lessons every business can learn from our experience. For the NSA, restoring public confidence was harder because the agency can't be completely open about what it does and doesn't do. The legal parameters within which it operates turned out to be a real hindrance.

Do you think companies appreciate the risks?
Companies underestimate the potential damage to their business when their reputation is compromised. Breaches can cause huge reputational harm. Make sure your entire organization is ready to manage that kind of damage – your legal staff, communications staff

7. HACKTIVISM (BREAKING INTO POP CULTURE)

Not all hackers are after money or sensitive information. Many businesses and governments find themselves targeted by "hacktivists" – attackers whose actions are politically motivated. These polarizing figures have also broken into pop culture. In 2014, actress Alyssa Milano published *Hacktivist*, a graphic novel that "questions the difference between good and evil in the age of technology." A year later, the TV show *Mr. Robot* premiered; its main character is a self-described "vigilante hacker."

ORI. BRYNN ALEXIS.
AND YOUR OCCUPATION?
CONVICT.
BEFORE YOUR CONVICTION.
I WAS A FIELD DIRECTOR FOR CIA'S PUBLICLY NON-EXISTENT CYBER COMMAND.
AND A MEMBER OF THE INTERNATIONAL CYBER ESPIONAGE COLLECTIVE KNOWN AS SVE_URS3LF.

ARTWORK: © 2016 ALYSSA MILANO. ALL RIGHTS RESERVED. USED WITH PERMISSION and business operations. They need to all be coordinated. Face the responsibility and own the problem. You want to be able to show that while your company may not be perfect, it can deal with the situation in the most responsible, forthright and transparent manner possible, both from a legal and a communications perspective.

How much do clients know about cybersecurity when they come to you for help?
One of the first discussions I'll have is about why the company might be attacked. There are many reasons why a business might be a target. Criminal groups try to get market-moving information that they can trade on, or other organizations connected to the business may have information the attackers want. They will often go through one business to get to another.

Increasingly, regulators are looking at data security in company supply chains. Contractual provisions need to be in place for managing cyber risk with all those business connections. Companies should exercise audit rights to ensure those parties are responsible stewards of their data.

When clients ask, "How do I protect myself against a cyber breach?" we explain that's just one element of a bigger strategy. Companies need to consider litigation risk, to structure their board of directors to oversee this risk, to manage increasingly complex compliance issues and to manage risk in their supply chain or cloud computing contracts. All of these issues have to be considered as part of an overall program.

What are the concerns you are hearing?
One is how to deal with the increasingly dynamic threat environment. The outlook is growing more complex on a daily basis, with the list of attackers including nation states, criminal groups and activists, and we see an increasingly complex regulatory and litigation landscape. Growing public awareness also increases pressure on companies across the board.

Companies want to know how to organize themselves. Legal affairs and information technology are relevant, but so are communications, human resources and just about every other department. The board has to be up to speed and able to ask the right questions. These concerns require a change in mindset. Cyber risk can't be solved overnight. It is a moving target in a landscape that is always changing and processes need to be in place to accommodate that reality.

How are cyber threats changing?
Ten years ago attacks were largely about stealing data, but they have evolved to a variety of more sophisticated and destructive goals and companies are being more open about their security and threats, so we have better information. We've seen distributed denial of service attacks where a lot of traffic is driven to a particular website to disrupt it. "Ransomware" is an important new threat, where an attacker locks data until a ransom is paid, often in digital currency. This raises complex legal and reputational issues. When is it appropriate to involve law enforcement? Can or should such attacks remain secret? How reliable is paying a ransom for restoring critical business functions? How will customers, shareholders, regulators and other stakeholders react to a company's response?

Does encryption have an important role?
The headlines have tended to paint encryption as a polarizing issue, something that can provide absolute security on the one hand and completely prevent law enforcement from doing its job on the other. But that really misses the point. Encryption is just one tool in a box of techniques. It is not a monolithic concept and its value depends on context. For example, the most secure encryption is not helpful if your employees do not know how to use it, or if the data it protects cannot be accessible to the business.

What should be a company's top priority?
Businesses typically get into trouble by giving the impression that they are not prepared. In this environment, everybody needs to be ready. Lack of preparation can damage a company's reputation. They might overreact, notifying the public or regulators before they know what actually happened. Or they may try to delay notification. That's not good and may not be legal.

Companies also need to show they have learned from prior incidents. Stakeholders understand that cybersecurity is a risk, but they have little tolerance for a company being hit twice in the same way.

SIOBHAN GORMAN is a Director in Brunswick's Washington, DC office and specializes in cybersecurity. She was formerly Intelligence and Cybersecurity Correspondent for *The Wall Street Journal*.

> “In this environment, everybody needs to be ready. Lack of preparation can damage a company's reputation”

RAJESH DE

As a Partner in global law firm Mayer Brown's Washington, DC office, Rajesh De leads its international Cybersecurity and Data Privacy practice. He returned to Mayer Brown in 2015 after serving as General Counsel at the US National Security Agency. De has held senior appointments in the White House, the Department of Justice and the Department of Defense, as well as in the intelligence community. He served as Counsel to the 9/11 Commission and to the Senate Homeland Security & Governmental Affairs Committee.

Safety in numbers

Cybersecurity could help promote the sharing of data for the public good, say Brunswick's MARIA FIGUEROA KÜPÇÜ and DAVID BROWN

CEOs may lie awake at night worrying about how to protect sensitive data. But some are also wondering if their data might contain answers to some of the world's most pressing problems.

Public expectations are growing for companies to be more responsive to the needs of the communities they serve. At the same time, the collection and analysis of data is increasingly fundamental to doing business in most sectors. Together with powerful recent advancements in technology, these pressures have opened a new frontier on the cybersecurity landscape, where the need to share data for the greater good must be balanced against the need to keep it safe.

"Data-driven insight offers an exciting opportunity to solve environmental and social challenges," says David Braunstein, Industry Solutions Innovation Lead, Global Business Services, IBM.

Data analysis technology is already being used to produce positive results for society, but relies on the sharing of data. Because of cybersecurity concerns, corporations are wary. A top priority for most is reassuring customers and stakeholders that their data is safe. Sharing data with outside organizations sits uneasily alongside that goal.

Every business that holds sensitive data faces this dilemma: reconciling the unease that stakeholders feel about cybersecurity with the results that can be achieved when data is used for the greater good – often for the benefit of those same stakeholders. But if the obstacles are large, the potential benefits for society are too big to ignore, and many companies are responding.

As they adopt more mature, confident cybersecurity policies, businesses should find they are able to share information more easily with like-minded companies, and discuss the best ways to use this precious resource to benefit themselves and their communities. That conversation can also help companies sharpen their thinking about the balance of security and transparency.

One coalition of global companies, Together for Safer Roads (TSR), hopes to demonstrate the benefits of companies pooling data for the greater good. The group formed to tackle growing, but largely preventable, traffic crash deaths and injuries – a problem identified by the United Nations as "a major health and development concern" in 2016. The private sector group's founding members include AIG, Anheuser-Busch InBev, AT&T, Chevron, Ericsson, Facebook, GM, IBM, iHeartMedia, Octo Telematics, PepsiCo, Republic Services, Ryder, UPS and Walmart.

"We accept traffic fatalities as inevitable because they're so common, but there's more that business can do to prevent them and save lives," says Scott Ratzan, Vice-President of Global Corporate Affairs at AB InBev and Governing Board Member of TSR. "Road safety is a business issue because it impacts our employees and their families, our operations and communities."

8. WATSON (THE NEXT LINE OF DEFENSE?)

Watson, the artificial intelligence technology developed by IBM (above), analyzes massive amounts of "unstructured" data – such as the blogs, videos, white papers, research reports and alerts that make up about 80 percent of the internet – to learn about and solve complex problems. Its huge brainpower has previously been applied to subjects ranging from healthcare to education and now, in partnership with eight universities, Watson will tackle cybersecurity. Once up to speed, it will interpret and bring context to this data and provide insights and recommendations to all levels of the cybersecurity industry, from novice analysts to the most advanced experts. "We're not going to stop the bad guys," says IBM's Charles Palmer, "but now we have a new lever to keep up … and maybe get ahead of them."

PHOTOGRAPH: THE WASHINGTON POST, GETTY

The World Health Organization estimates that 1.25 million people are killed in crashes each year – a rate of more than two per minute – and up to 50 million are injured in collisions. Motorized traffic is increasing with population growth and urbanization. If current trends continue, by 2030 crashes will be ranked seventh as a cause of death globally, up from ninth position now.

Crash injuries disproportionately impact young people and those in developing countries. In addition to human suffering, traffic crashes can cost between 1 and 1.5 percent of a country's GDP. For some economies, those losses exceed the amount received in development aid.

To tackle the problem, the UN proposes improvements to road design and repairs; safety features on vehicles; changing driver behavior through policing and public information campaigns; improved care for victims; and better public transportation. The UN *Global Plan for the Decade of Action for Road Safety* outlines its goal "to stabilize and then reduce the forecast level of road traffic fatalities around the world" by 2020.

> **"As they adopt more mature, confident cybersecurity policies, businesses should find they are able to share information more easily with like-minded companies"**

"The private sector can bring innovation and scale to proven strategies that will help to achieve the goals of improving traffic safety outlined by the UN," Ratzan says.

Public-private partnerships involving data and technology are already reshaping societies around the world. In Brazil, "intelligent" transportation systems are being launched, while IBM's "Smarter Cities" initiative is working with the government of Vizag, India, a city plagued by cyclones and floods, to improve emergency response efforts. A large Smart City program in Barcelona is redefining its public services, using data to improve quality of life for its citizens.

That trend to use data to improve society sets a precedent for TSR member companies, many of which have data that would be helpful to share. AB InBev and UPS, for instance, have first-hand knowledge of road conditions from large fleets of delivery vehicles. AT&T has aggregated data that it has used in its "It Can Wait" initiative, a social media campaign to curb the dangerous practice of texting and driving. IBM, which owns The Weather Channel, has extensive meteorological data. And AIG has broad insights gained from decades of insurance claims across its global network.

"We pay out about $130 million each work day in claims, from very small to very large, and we learn something from every one," says Rob Schimek, Executive Vice-President and CEO, Commercial, AIG.

TSR is optimistic, but cautious about finding ways to combine such knowledge to potentially save lives. Member companies are stewards of sensitive and proprietary data and each data source has its own cybersecurity issues of privacy and risk. Technical issues that would allow the data to be accessible on multiple platforms may also need to be addressed. However, Braunstein sees more companies willing to explore the possibilities.

"Now we have the data analytics capabilities," he says. "There are some near-term gains we can already see. Bringing together or even blending cross-sector approaches will take time – but we're very excited to try."

MARIA FIGUEROA KÜPÇÜ is a Partner and Head of Brunswick's New York office. She leads the US Business and Society practice. **DAVID BROWN** is an Associate in Washington, DC, and advises on regulatory and public affairs, cybersecurity, and crisis communications.

9. PANAMA PAPERS (PRIVATE TO PUBLIC)

In an audacious leak that revealed the offshore bank accounts of business figures, celebrities and world leaders, more than 11.5 million documents held by Panama-based law firm Mossack Fonseca were divulged to the International Consortium of Investigative Journalists in early 2016. The documents – roughly 10 million more than were revealed by Edward Snowden – are still being reviewed, but have already made an impact. Iceland's Prime Minister Sigmundur Davíð Gunnlaugsson stepped down after his holdings were published, while some of the world's largest banks are being investigated. The source of the leak has used encryption to remain anonymous.

PHOTOGRAPH: RODRIGO ARANGUA, GETTY

A policy on risk

The cyber insurance industry is holding companies to a high standard, say Brunswick's WENDEL VERBEEK and SOFIA MATA-LECLERC

A spate of high-profile breaches in recent years has led to a booming market for cyber insurance. PwC predicts the global market will reach $7.5 billion by 2020. That kind of growth brings considerable influence and is making the insurance industry a significant force that is reshaping expectations for companies around cybersecurity preparedness.

"Three years ago, cyber insurance wasn't that common," says Kristy Harris, Manager of Corporate Insurance at Southwest Airlines. "It's now come to the forefront in response to these high-profile breaches."

According to Moody's Investors Service, more than 50 insurers globally offer standalone cyber coverage. That number is expected to grow as companies, and by extension underwriters, increasingly focus on mitigating the risks associated with a breach.

In some cases, underwriters have had to scramble to catch up with their clients in understanding the complex operations that make cybersecurity protection effective. Increasingly, however, cyber insurers themselves are driving the discussion, wanting more sophisticated security plans tailored to each company's risk profile.

"A few years ago when we were talking to cyber insurance underwriters, we found that some didn't differentiate between company business models, or take into account the different risks," Harris says. "They have come a long way since then. They are learning to underwrite the risk better, getting more comfortable assessing risk. And we're seeing more expansive coverage as a result."

Data breach insurance is fairly narrowly defined, but can cover forensics, communications and legal support, network interruptions, and fallout from lawsuits. "People think cyber insurance will help cover anything digital, but that's not the case," says Harris. "The big 'a-ha' moment for us at Southwest was trying to insure against someone stealing our loyalty reward points. Theft of assets is a crime loss – not a cyber loss. Psychological cons and impersonation losses aren't covered either."

> "Tell me more about how you are addressing risks culturally as you go. I am looking for companies who are investing in – and changing – behavior"
>
> MARCUS BREESE
> Hiscox London Market

Insurers' expectations are helping to drive cyber policy for companies. One of the first things a cyber underwriter will want to see is a security incident response plan that goes well beyond IT. Specific levels of responsibility should be included, with triggers to ensure the right people are involved at the right time.

"I get concerned when it seems that a client's IT guys are kept completely separate, in a dark dungeon somewhere," says Laila Khudairi, Head of Cyber at insurer Tokio Marine Kiln. "In the event of a breach, there may not be a proper escalation process."

An effective cybersecurity plan needs to be able to involve the entire company, says Marcus Breese, Cyber and Professions Line Underwriter for Hiscox London Market. "Tell me more about how you are addressing risks culturally as you go," he says. "I am looking for companies that are investing in – and changing – behavior."

It is critical that insurers see multiple stakeholder perspectives represented – customers in particular. If affected parties feel they have been treated well, they are less likely to sue or to take their business elsewhere, Khudairi says.

Since cyber's risk landscape shifts constantly, a security plan needs to be regularly put through its paces, says Erica Constance, Senior Vice-President and cyber expert at Paragon International Insurance Brokers in London. "I would expect companies to test these procedures annually, at least," she says. "Things are going to change."

Regulation is one area that is already changing. The 1998 UK Data Protection Act "was created before the first text was sent, so it doesn't take into account that our lives are now played out online," Constance says. In 2018, the EU General Data Protection Regulation will come into effect, and companies active in Europe will be required to report certain breaches and review their practices.

All the pressures companies face are echoed by cyber insurers. "Crisis communications preparedness is a larger consideration, and it affects more than the policy's premium," Khudairi says. "It ultimately determines whether or not we will underwrite the risk."

WENDEL VERBEEK is a Director in Brunswick's London office advising on financial and crisis communications. **SOFIA MATA-LECLERC** is a Director in San Francisco, specializing in crisis, cybersecurity and corporate reputation.

Nailing security

With creativity and communications, AVON is building a "human firewall" around its data. Brunswick's GIOVANNA FALBO and PHIL MORLEY report

With almost 30,000 Associates around the world, international beauty company Avon coordinates a network of millions of direct sellers and many millions more customers. Increasingly, all that activity is on digital and online platforms, raising the company's need not just for basic data privacy rules, but for a leadership role on cybersecurity awareness.

CEO Sheri McCoy and her team recently launched Be CyberSafe, an internal campaign to build a "human firewall" around Avon's data. In a roll-out video, McCoy says, "Our business is built on trust. It's at the heart of everything we do."

Building on that trust, the company's goal was to move the topic of cybersecurity from a shadowy liability to a strong, visible asset. The best way to do that was by empowering the business's Associates at work and at home. Everyone has an email address or mobile phone and can benefit from learning how to make their information more secure.

> "We want to shift the mindset from compliance to commitment. To do that, the key lever to pull is creativity"
>
> SHERI McCOY, Avon CEO

Behind Avon's initiative are studies that show breaches are often triggered not through a weakness in tech defenses, but through employee error. PwC reports that worker actions led to about a third of all breaches in 2015. Others put that figure much higher.

Lost laptops, phones or USB drives, duplicated passwords, and clicks on links that contain a virus are some of the more common lapses. In one striking and increasingly frequent scam, some companies have lost amounts into the millions of US dollars when an employee, complying with what appears to be an email from their CEO, delivers funds to a fraudulent account.

SINCE EMPLOYEES are on the cybersecurity front line, they are positioned to become a company's first and arguably best line of defense. Former New York City Police Commissioner Ray Kelly, now Vice-Chairman at investigative consultancy K2 Intelligence, said in a recent interview in *The Wall Street Journal* that companies can do more to stop intrusions caused by "employee carelessness" by initiating "robust training programs."

For Avon, this meant creative communications involving wit, memorable messages and strong visuals, all to humanize the topic.

IN PURSUING ACTIVE engagement on cyber safety within all parts of the company, the Avon team knew from the outset that it had to change not just what Associates think about cybersecurity, but how they feel about it in order for the messages to sink in. That required an inspired campaign, with as much thought about graphic design and presentation as message content.

Cybersecurity is often viewed as a dull and dry subject. The team knew it would have to distill the campaign's messages and use a creative approach in order to strike the right balance of advice and accessibility. "Creativity is needed to engage people emotionally," McCoy says. "We want to shift the mindset from compliance to commitment. To do that, the key lever to pull is creativity."

The Be CyberSafe campaign used the color yellow, associated with caution, on posters and in videos, some of which featured distinctive yellow nail polish. "In the end, it had all the attributes we want in our brand: witty, warm and welcoming," McCoy says. "The idea behind the yellow nail polish was to illustrate, in a creative, playful way, that cybersecurity was literally in the hands of our Associates."

In the roll-out video, McCoy painted her own nails the campaign's signature yellow to address the company. The moment clearly positioned the campaign as a company priority, while at the same time setting a lighter tone that helped secure everyone's involvement.

Associates were encouraged to take part in a "Polish Pledge," painting their own nails at work. The activity became a cornerstone of the campaign, highlighting its messages and creating a viral awareness as office talk naturally turned to the brightly painted nails. Associates posed for photos and posted them on Yammer. As part of the normal workday, the activity served to acknowledge and accommodate Associates' busy schedules, while still breaking through the volume and frequency of their normal communications.

Published on multiple channels, the team worked hard to simplify the cybersecurity message, avoiding tech jargon and focusing instead on basic behaviors, broken into four themes: general awareness, appropriate email use, safe online browsing and protecting sensitive information.

Even in the campaign's early stages, Avon's surveys showed a 15 percent increase in the perception of cybersecurity as the responsibility of individuals rather than the IT department.

A big part of the Be CyberSafe campaign reminds Associates how to keep personal information – not just company data – safe and secure through awareness and good habits.

"Associates are just as vulnerable at home as at work," McCoy says. "With these steps, they've learned how they can protect themselves, and the company, in both areas of their lives."

GIOVANNA FALBO, a Partner in Brunswick's New York office, leads the US Employee Engagement practice. **PHIL MORLEY** is Director of Employee Engagement at the firm's creative agency, MerchantCantos. Additional reporting by **ELEANOR FRENCH**, an Associate in New York.

Avon's cybersecurity awareness campaign features yellow nail polish, the color chosen for its association with caution. In a video featuring CEO Sheri McCoy and in posters, Associates are reminded that cyber responsibility is in their hands

Be
cyber
sophisticated
Trust
is
critical
It's
in
our
hands
Be CyberSavvy
Protect
yourself
online
Be CyberSafe

IMAGES COURTESY AVON

You can travel but you can’t hide

Trouble on your business trip is only a click away, says THOMAS PARENTY

Keeping sensitive information safe during business travel used to be simple. Handcuff a briefcase to your wrist, wear a dark suit and sunglasses, and have a healthy supply of exploding pens and invisible ink.

Today, with cybersecurity top of mind, the savvy business traveler is advised to carry a burner phone, use a loaner laptop, avoid email or Wi-Fi, and not carry a mobile phone into meetings.

The advice could very well include saving money on the plane ticket and not going at all. Yes, the risks are real and significant, but should you wish to do anything remotely productive while traveling, they are also unavoidable.

All a cyber attack does is exploit known risks – risks for which there are known countermeasures. If you go out in a rainstorm without a coat or umbrella you’ll get wet. However, with a few simple tools you can go outside without looking like a drenched cat. The same principle applies to cybersecurity.

The first lesson is that you can’t trust the network. All email and web browsing can be intercepted by anyone in the vicinity of an airport lounge or café where you use Wi-Fi. Your hotel can access any communication channeled through its network, and anything you’ve sent or downloaded on a local data plan is equally accessible. Your emails back to HQ might not be of as much interest as a world leader’s, but still, you have some pretty valuable secrets, right?

Use a virtual private network (VPN). This can be either a business VPN tied to your corporate network or a personal one that connects to a server in the country of your choice. Added bonus: you can bypass any local bans of sites such as Facebook, YouTube and Netflix.

Similarly, every phone call and text that you send will go through networks that can be monitored. Encryption may provide the answer. FaceTime and WhatsApp are encrypted by default. Alternatives include Silent Circle and Open Whisper Systems.

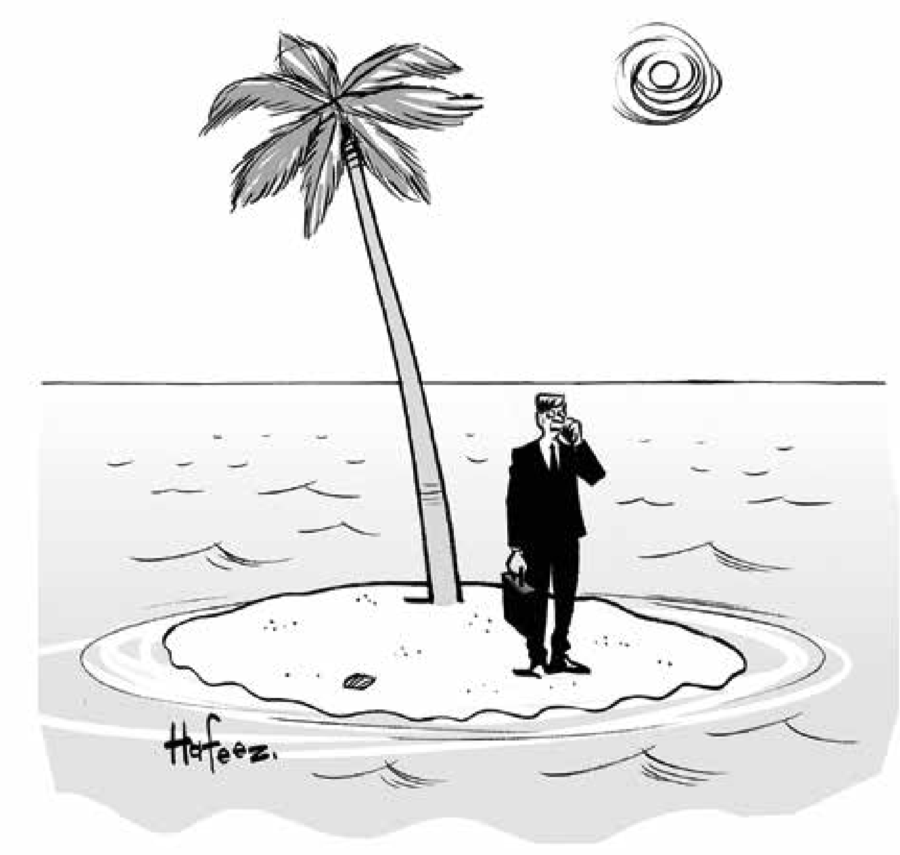
For those who are gifted at leaving phones on airplanes or laptops in hotels, talk to your IT department about enabling whole-disk encryption on your hardware. It will render your information gibberish should someone copy it. For the increasingly paranoid, ask them to set a “BIOS” password – this will bolster the security of your operating system.

Think a nation state might be after you? Use a laptop with a bad maintenance rating. The harder it is to fix, the harder it is to put an evil chip into it.

In addition to having anti-virus software, update your software before your trip and don’t install any updates while you’re on the road. They can make you vulnerable.

Another threat is malicious software. Once on your device it can do whatever it likes, stealing or destroying your information, or surreptitiously turning on the camera and microphone. As a last resort, don’t do anything in front of your devices you wouldn’t want a cyber attacker to witness. It’s probably best to leave the handcuffs at home, or at the very least, on the briefcase.

A veteran of the US National Security Agency, **THOMAS PARENTY** runs a consultancy advising global businesses on information security.



“OK, go ahead. I’m on a private network.”

CARTOON: KAAMRAN HAFEEZ

Read on.

www.brunswickgroup.com/review

To download and share
Brunswick Review stories go to
www.brunswickgroup.com/review
Download the iPad app at
www.brunswickgroup.com/review/app
You can follow us on Twitter
@BrunswickReview
Highlights from this and previous
issues are also available on LinkedIn

Brunswick Group offices

ABU DHABI
Office 506
Park Rotana Office Complex
Twofour54
PO Box 77800
Abu Dhabi
United Arab Emirates
T: +971 2 234 4600
uaeoffice@brunswickgroup.com

BEIJING
2605 Twin Towers (East)
B12 Jianguomenwai Avenue
Beijing, 100022
People's Republic of China
T: +86 10 5960 8600
beijingoffice@brunswickgroup.com

BERLIN
Taubenstraße 20-22
10117 Berlin
Germany
T: +49 30 2067 3360
F: +49 30 2067 3366
berlinoffice@brunswickgroup.com

BRUSSELS
Avenue des Arts 27
1040 Brussels
Belgium
T: +32 2 235 6510
F: +32 2 235 6522
brusselsoffice@brunswickgroup.com

DALLAS
200 Crescent Court
Suite 225
Dallas, TX 75201
USA
T: +1 214 254 3790
F: +1 214 254 3791
dallasoffice@brunswickgroup.com

DUBAI
Level 5
Gate Village Building 10
PO Box 506691
Dubai International
Financial Centre
Dubai
United Arab Emirates
T: +971 4 446 6270
F: +971 4 436 4160
uaeoffice@brunswickgroup.com

FRANKFURT
Thurn-und-Taxis-Platz 6
60313 Frankfurt am Main
Germany
T: +49 69 2400 5510
F: +49 69 2400 5555
frankfurtoffice@brunswickgroup.com

HONG KONG
12/F Dina House
11 Duddell Street, Central
Hong Kong SAR
T: +852 3512 5000
F: +852 2259 9008
hongkongoffice@brunswickgroup.com

JOHANNESBURG
23 Fricker Road
Illovo Boulevard, Illovo
Johannesburg
South Africa
T: +27 11 502 7300
F: +27 11 268 5747
johannesburgoffice
@brunswickgroup.co.za

LONDON
16 Lincoln's Inn Fields
London WC2A 3ED
United Kingdom
T: +44 20 7404 5959
F: +44 20 7831 2823
londonoffice@brunswickgroup.com

MILAN
Via Solferino, 7
20121 Milan
Italy
T: +39 02 9288 6200
F: +39 02 9288 6214
milanoffice@brunswickgroup.com

MUMBAI
The Capital
814, 8th Floor
C-70, G Block, Bandra Kurla Complex
Bandra East
Mumbai 400 051
Maharashtra
India
T: +91 22 61358500
mumbaioffice@brunswickgroup.com

MUNICH
Widenmayerstraße 16
80538 Munich
Germany
T: +49 89 809 90 250
F: +49 89 809 90 2555
munichoffice@brunswickgroup.com

NEW YORK
245 Park Avenue
14th Floor
New York, NY 10167
USA
T: +1 212 333 3810
F: +1 212 333 3811
newyorkoffice@brunswickgroup.com

PARIS
69 Boulevard Haussmann, 6th Floor
75008 Paris
France
T: +33 1 53 96 83 83
F: +33 1 53 96 83 96
parisoffice@brunswickgroup.com

ROME
Piazza del Popolo, 18
00187 Rome
Italy
T: +39 06 36712806
F: +39 348 7098590
romeoffice@brunswickgroup.com

SAN FRANCISCO
One Bush Street
Suite 1400
San Francisco, CA 94104
USA
T: +1 415 671 7676
F: +1 415 671 7677
sanfranciscooffice
@brunswickgroup.com

SÃO PAULO
Avenida Dr. Cardoso de Melo
1.340 - Sala 42
Vila Olimpia
São Paulo SP
Brasil 04548-004
T: +55 11 3076 7620
saopaulooffice@brunswickgroup.com

SHANGHAI
Room 2907,
United Plaza
1468 Nan Jing Road West
Jing'an District
Shanghai 200040
People's Republic of China
T: +86 21 6039 6388
shanghaioffice@brunswickgroup.com

SINGAPORE
6 Battery Road
#15-05 Singapore 049909
T: +65 6426 8188
F: +65 6426 8199
singaporeoffice@brunswickgroup.com

STOCKHOLM
Fourth Floor
Birger Jarlsgatan 15
111 45 Stockholm
Sweden
T: +46 8 410 32 180
F: +46 8 611 00 56
stockholmoffice@brunswickgroup.com

VIENNA
Concordia Haus
Bankgasse 8
1010 Vienna
Austria
T: +43 1 907 65 10
F: +43 1 907 65 10 40
viennaoffice@brunswickgroup.com

WASHINGTON, DC
1099 New York Avenue, NW
Suite 300
Washington, DC 20001
USA
T: +1 202 393 7337
F: +1 202 898 1588
washingtonoffice@brunswickgroup.com

Brunswick Group companies

BRUNSWICK ARTS
16 Lincoln's Inn Fields
London WC2A 3ED
United Kingdom
T: +44 20 7936 1290
F: +44 20 7936 1299
bartsinfo@brunswickgroup.com
www.brunswickarts.com

MERCHANTCANTOS
20 Lincoln's Inn Fields
London WC2A 3ED
United Kingdom
T: +44 20 7242 1336
F: +44 20 7936 7788
office@merchantcantos.com
www.merchantcantos.com

THE LINCOLN CENTRE
18 Lincoln's Inn Fields
London WC2A 3ED
United Kingdom
T: +44 20 7936 1300
F: +44 20 7396 3535
info@thelincolncentre.co.uk
www.thelincolncentre.co.uk

BRUNSWICK GROUP LLP
www.brunswickgroup.com/review