accenturestrategy

SECURING THE DIGITAL ECONOMY

Reinventing the Internet for Trust

INTO THE NEW

CONTENTS

Authors

Omar Abbosh

Group Chief Executive, Accenture
Communications, Media & Technology

Omar is responsible for the company's US$8 billion business serving the digital platforms, media, telecommunications, semiconductor and consumer electronics industries. Omar brings three decades of experience to his role, and his experience and deep connections in Silicon Valley enable him to stay ahead of key shifts across multiple technologies.

Kelly Bissell

Senior Managing Director,
Accenture Security

Kelly leads the company's US$2 billion security business across all industries. As a recognized cybersecurity expert, Kelly specializes in incident response, identity management, privacy and data protection, secure software development, and cyber risk management.

Kelly's vision is to help businesses embed security in everything they do.

除《企业家第一课》、《企业家功成堂》外，其他公众号分享本期资料的，均属于抄袭！

邀请各位读者朋友尊重劳动成果，关注搜索正版号：《企业家第一课》、《企业家功成堂》

谢谢观看！

企业家第一课，专注做最纯粹的知识共享平台

关注官方微信
获取更多干货

加入知识共享平台
一次付费 一年干货

Building on Trust

When a person creates an online account, makes a purchase from a website or downloads an app, it's not just the exchange of data, goods or services taking place.

It's a transaction in the ultimate currency: trust.

Today, there is a real risk that trust in the digital economy is eroding.

Why? The once open, global Internet has outgrown its original purpose as a communication and information-sharing tool. As the Internet has become more complex, digitally fueled innovation has outpaced the ability to introduce adequate safeguards against cybercriminals.

Unless business leaders take effective action, there is a real risk that this lack of safeguards could reduce the growth of the entire digital economy, hurting both individual companies and the economy as a whole.

CEOs are aware of the problem and have increased spending on cybersecurity in response to escalating cyberthreats. Companies have handled many threats with markedly successful results, but their efforts have not solved the larger problem of Internet fragility.

Attackers need only a single lucky strike, while defenders must be constantly vigilant against any potential type of incursion.

The fragile nature of the Internet is putting the value of the digital economy at risk, which is why CEOs need to end their piecemeal approach and put trust and security at the forefront of business strategy.

In an analysis we conducted with 30 leading technologists, and additional fieldwork with 1,700 C-level executives, we uncovered concrete actions CEOs can take to begin the crucial work of securing the digital economy.

For a practical framework that can help safeguard the Internet's future, leaders should look to an analogy from the oil and gas industry. Oil and gas executives spend much of their time determining how to maximize production—which often means focusing on the engineering and technology solutions that largely operate "below ground."

However, innovative extractive technologies are only part of the equation. Executives also have to address the many challenges related to business and operating models, strategy, politics and economics that exist "above ground."

Similarly, securing the digital economy will take more than fixing Internet technology and network issues below ground. There are also clear opportunities for CEOs to step up on the above-ground business initiatives.

So, what can business leaders do above ground? CEOs can own and drive a secure Internet as a critical component of their business strategies. One key above-ground action would be improving *governance*.

CEOs need to join forces with other top executives, government leaders and regulators to develop principle-based standards and policies to safeguard the Internet.

Another above-ground action CEOs can take is steering what we call *business architecture*—a company's own business model and value chain—in a direction that makes their own enterprise secure. Examples of actions that can be taken include committing to giving data access only to people who need it and who have the right credentials. Importantly, they should extend their commitment to making their own enterprise secure to their partners, applying the same standards to their entire business ecosystem.

And they should ensure that the very idea of a trusted digital economy is embedded in all future business models.

To some CEOs, above-ground decision-making opportunities may seem more accessible than below-ground choices, but leadership is needed in both, even from CEOs outside the technology sector. All CEOs also have the opportunity to influence and inspire technology infrastructure investments below ground. By making decisions to update everything from devices to cables and networks, CEOs can support the complexity and connectivity of today's Internet while also promoting security.

These *technology* decisions present the third concrete way CEOs can proactively secure the digital economy. CEOs should embrace new technologies that can advance their businesses and enhance digital safety. Meanwhile, they should elevate their understanding of how the same technologies can introduce unintended vulnerabilities.

But the CEOs whose businesses focus on the Internet itself have an even greater responsibility: They can concentrate explicitly on promoting innovation in the Internet's infrastructure. Their actions resolve inherent vulnerabilities, enable growth and prepare for the advent of quantum computing, which will present new opportunities and threats.

Building a trustworthy digital economy will take decisive—and, at times, unconventional—leadership from the C-suite. Where should they start? By working collaboratively with each other. If they follow the roadmap detailed on page 7, leaders could bring back the confidence needed in the Internet for individuals, organizations and societies to innovate and grow.

Governance:

Join Forces with Other Companies and Govern Globally

74 percent of business leaders say solving the cybersecurity challenges of the Internet economy will require an organized group effort.

Business Architecture:

Connect and Protect with a Model Run on Digital Trust

80 percent of business leaders say protecting companies from weaknesses in third parties is increasingly difficult given the complexity of today's sprawling Internet ecosystems.

Technology:

Advance Business and Enhance Safety

79 percent of business leaders say the rate of technology adoption and innovation has outpaced the security features needed to ensure a resilient digital economy.

ABOVE GROUND

Standards and Best Practices

BELOW GROUND

Technology Investments

How Leaders Can Address Internet Security:

Above ground, the strategic initiatives of CEOs can lead to standards and best practices. *Below ground,* through innovative technology improvements, CEOs can invest in improving the Internet's infrastructure.

WHY THE INTERNET CAN'T SUSTAIN THE DIGITAL ECONOMY

Without trust, the future of our digital economy and its nearly limitless potential is in peril. Piecemeal efforts to address cybersecurity issues—including the Internet's inherent flaws, vulnerabilities from the Internet of Things (IoT), identity and data veracity and increasing digital fragmentation—have fallen short. Through their decisions above ground on industry-wide governance and their business architecture and technology infrastructure below ground, however, CEOs can have the influence necessary to collaboratively address these overarching issues.

Many of the issues affecting today's Internet are due in part to its rapid growth in both users and applications. The entire digital economy is now dependent on the Internet. At the same time, while businesses, individuals and societies are increasingly connected, those connections are also becoming more complex.

In 2007, there were 1.2 billion Internet users. In 2017, there were 4.2 billion—more than half of the global population.[1]

The number of IoT-connected devices will likely reach 25 billion by 2021.[2]

By 2024, Long-Term Evolution (LTE) networks (also called 4G) will cover an estimated 90 percent of the population, with 5G networks covering about 40 percent.[3]

Handling these connections requires more lines of code, more data and more capacity. Without a more resilient and trustworthy Internet, a single breach can have serious, cascading effects. For example, the 2017 NotPetya cyberattack cost Maersk more than US$300 million, and the damages to all other companies affected totaled more than US$10 billion.[4]

Against this backdrop, with computers and networks so deeply embedded in critical infrastructure such as water supply and public health systems, the risks to both the economy and public safety are high.

Consider the impact of the 2017 WannaCry cyberattack on the United Kingdom National Health Service (NHS). It led to the cancellation of 19,000 appointments and the diversion of ambulances, and ultimately cost almost £100 million.[5]

Yet 79 percent of our respondents reported that their organization is adopting new and emerging technologies faster than they can address related security issues.

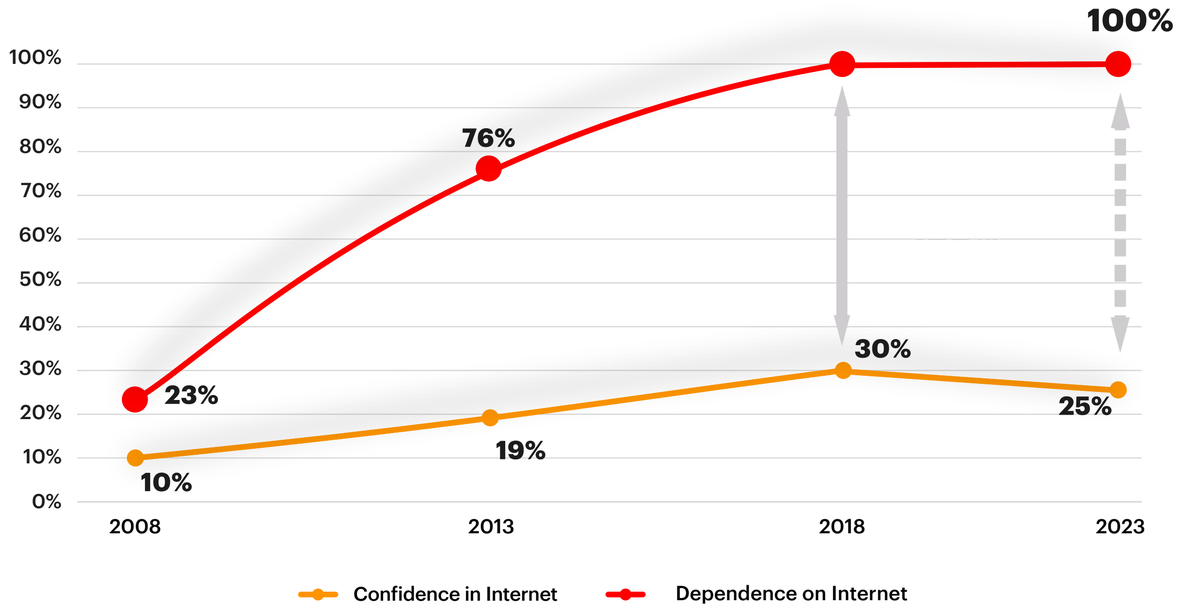


Exhibit 1: Dependence on the Internet is Growing While Confidence in Internet Security is Low and Forecast to Drop to 25 percent Over the Next Five Years.

Source: Accenture Research

Even as 68 percent of CEOs report that their businesses' dependence on the Internet is increasing, they acknowledge that their confidence in Internet security, already low at 30 percent, will drop even lower if nothing changes to improve it. In the next five years, the confidence level in the Internet is forecast to drop to 25 percent, while dependence on it is assumed to remain at 100 percent. *(See Exhibit 1).*

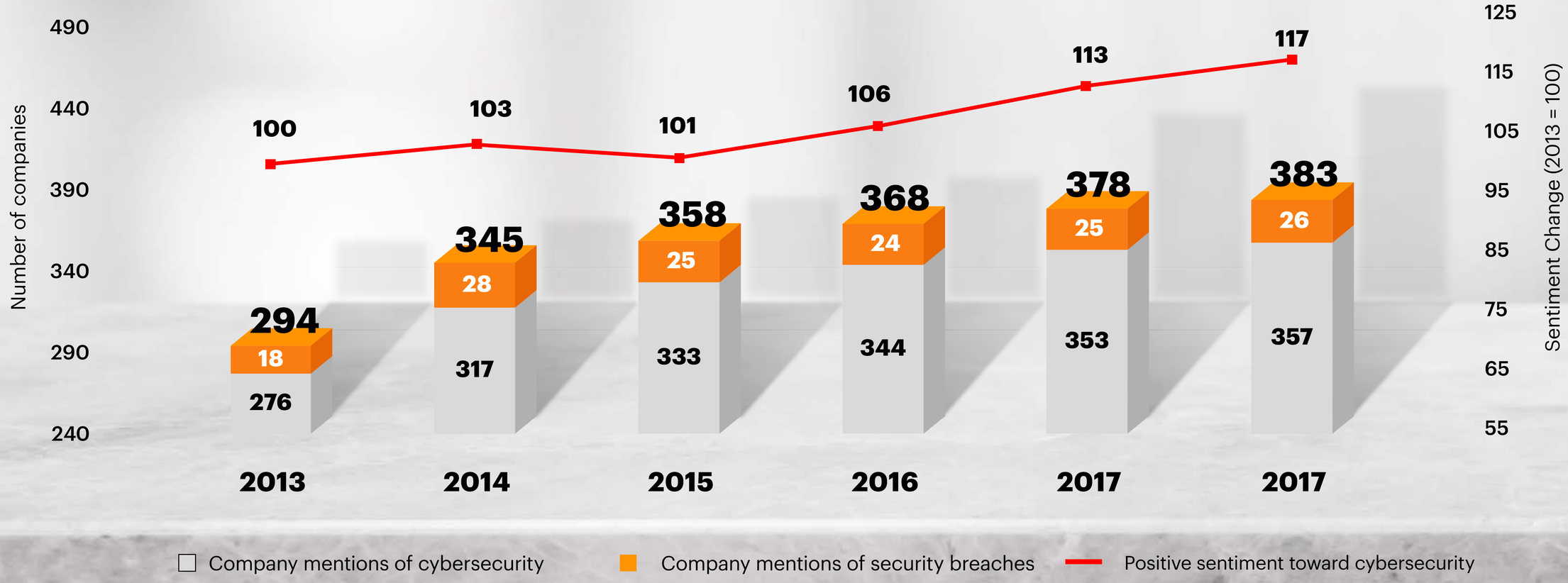
Nearly 80 percent of the S&P 500 companies in our analysis have also mentioned cybersecurity initiatives during recent earnings calls.[6]

Five years ago, that figure was just slightly more than 50 percent.

As the Internet's fault lines are becoming more apparent, companies are trying to build trust equity and are publicly discussing ways to do so.

However, only a relatively small percentage of companies are willing to openly discuss breaches—an above-ground issue that CEOs need to address. *(See Exhibit 2).*

Exhibit 2: S&P 500 CEO Sentiment Toward Cybersecurity (Based on Transcripts from 11,418 Earnings Calls)



Note: Each year is computed as trailing 12 months from September of the previous year to August of the current year. For example, 2018 includes data from September 2017 to August 2018.

Source: Accenture Research

The Internet Just Can't Keep Up

How did today's problems of Internet security originate? The Internet was not initially designed to address issues like perpetually increasing levels of complexity and connectivity. It was developed to enable high levels of data sharing, which requires trust.

Researchers during the Cold War aimed to build a trusted communications network underground that could withstand a nuclear attack. Their concerns did not include preventing cyberattacks, largely because modern forms of cyberattack did not exist at the time.

As the Internet evolved from a military asset to an open infrastructure, security considerations, such as they were, focused on preventing physical failures.

Today, many of the base Internet protocols—the set of rules embedded in code so all machines on a network or series of interconnected networks "speak" the same language—are unfit for current demands and are insecure. This has led to increasing challenges below ground that CEOs should address.

Consider the Border Gateway Protocol (BGP), a protocol that has been in use since 1994. BGP routes traffic through cables and connections among services providers, countries and continents. But BGP traffic is vulnerable in transit. In 2017, traffic to and from 80 Internet service providers (ISPs) was briefly routed to an unknown Russian operator, showing how easy it is to reroute information, whether intentionally or accidentally.[7]

Other systems widely utilized on the Internet, such as the Domain Name System (DNS) and the Public Key Infrastructure (PKI), which underpins much of the encryption utilized on the Internet today, are similarly vulnerable to potential attacks.

The IoT Effect

More recently, the rise of the IoT has expanded the surface area of attack for enterprise networks from thousands of end points—including remote devices, such as mobile phones and laptops—to several million for the largest companies.

At the same time, the IoT compels all companies to suddenly manage what are often unfamiliar technology processes, where every connected device is a potential vulnerability.

Take the case of an attack suffered by a North American casino.

The casino had an Internet-connected fish tank that fed the fish automatically and monitored their environment.

Hackers managed to use the fish tank's connection to break into the fish tank monitor and then use this as an entry point into the company's systems.

The data was then sent to hackers in Finland.[8]

While the IoT has increased digital capabilities, improved efficiencies and unleashed growth opportunities for a wide variety of industries, it has also suddenly created complexity for all businesses, leaving them more vulnerable.

Identities in Crisis

The “most fundamental challenge” facing business and society is around identity, according to Amit Mital, founder of Kernel Labs and former chief technology officer (CTO) at Symantec. But the challenge of authenticating identities and confirming the integrity of data on the Internet also presents a key opportunity for the C-suite to renew trust in the digital economy.

Mital comments: “No individual has a single identity that they use in the digital world. This fragmentation requires too much effort for the individual to ensure consistency, reliability and security. As a service provider, if I cannot trust in the digital identity of a person, then that precludes me from providing services that I might want to provide, or risk providing services to someone who has stolen another’s identity.”

Most individuals who use the Internet have multiple online identities; the average Internet user today manages 27 passwords, up from six in 2006.[9]

In this environment of content over context, Internet users have less ability to ascertain the origin of material they access and whether it is valid. Facebook, for example, closed nearly 300 million accounts, or 14 percent of all accounts, in 2018 after determining that they were fake.[10]

And although 79 percent of the executives we surveyed believe companies are basing their most critical strategies on data, many have not invested in the capabilities needed to verify that data.

None of us really know what’s happening out there. We have no idea how our data is being used. I think that’s the key issue and we’re [only] seeing the tip of the iceberg with recent data breaches being announced.”

Norman Frankel, chairman of the UK-based iCyber-Security Group

No Flow Versus Free Flow

The Problem of Digital Fragmentation

Another key challenge that demands the attention of CEOs is the increasing fragmentation of the Internet.

This trend, fueled in part by security concerns, could by itself stunt future global economic growth. *Walled gardens*—isolated, secured information systems—are proliferating as countries and regions limit the free flow of data across borders through regulations.

Already 13 countries, accounting for 58 percent of the global GDP, have some version of these regulations.[11] Heightened concerns about borderless cyberattacks, coupled with geopolitical tensions, threaten to result in even greater restrictions. *(See Exhibit 3).*

Business leaders are already dealing with this reality as they tailor global operating models to countries with more restrictions.

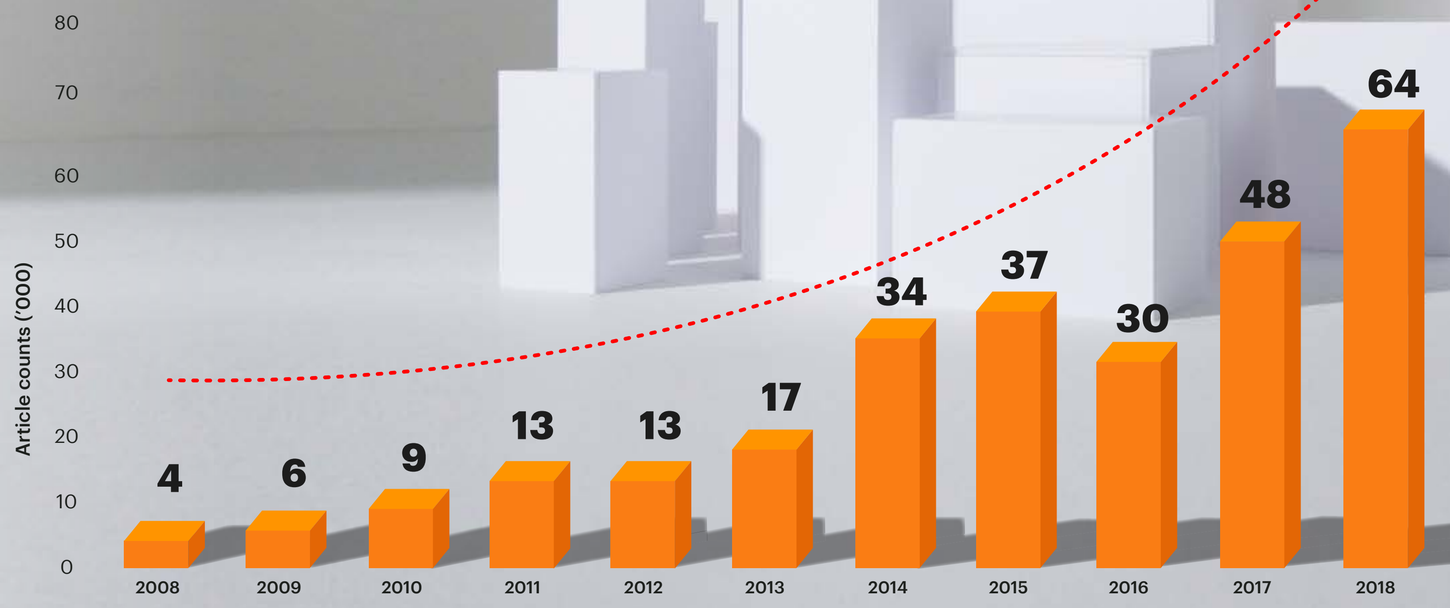


Exhibit 3: Digital Fragmentation Media Coverage

Source: Factiva and Accenture Research Analysis. Factiva search based only on "digital fragmentation", "splInternet", "balkanization", "Internet balkanization", "cyber war", "cyber attack", "data breach", "data leak", "cyber threat", "cyberthreat" as keywords among major global business publications.

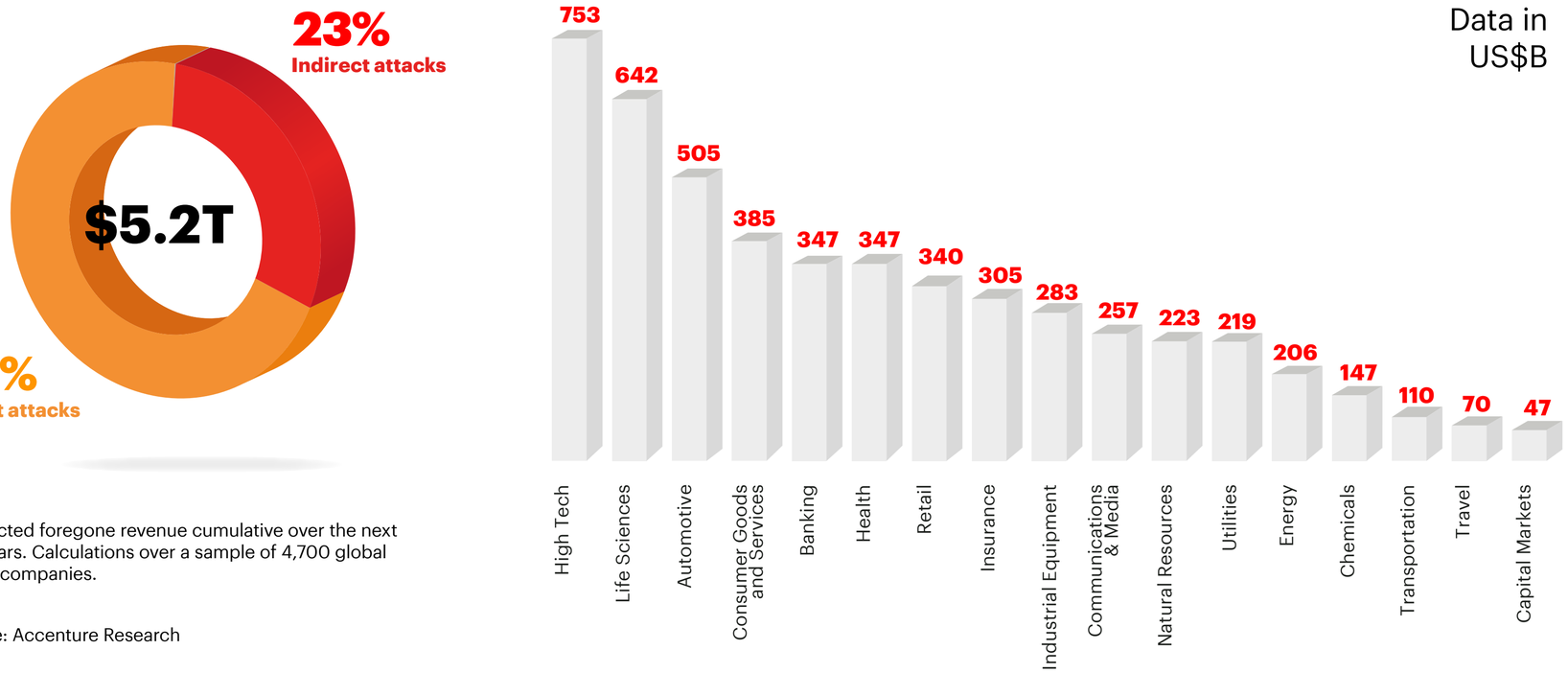
The Cost of Insecurity

For CEOs, one of the most glaring challenges of an insecure Internet is the economic cost.

In the private sector, over the next five years companies risk losing an estimated US$5.2 trillion in value creation opportunities from the digital economy—almost the size of the economies of France, Italy and Spain combined—to cybersecurity attacks. *(See Exhibit 4).*

This translates to 2.8 percent in lost revenue growth for the next five years for a large global company. High-tech industries face the highest risk, with more than US$753 billion hanging in the balance.

Exhibit 4: Value at Risk* by Industry—Direct and Indirect Attacks (Cumulative 2019 to 2023, US$ Billion)



* Expected foregone revenue cumulative over the next five years. Calculations over a sample of 4,700 global public companies.

Source: Accenture Research

Keeping Tabs on Cybersecurity Investments

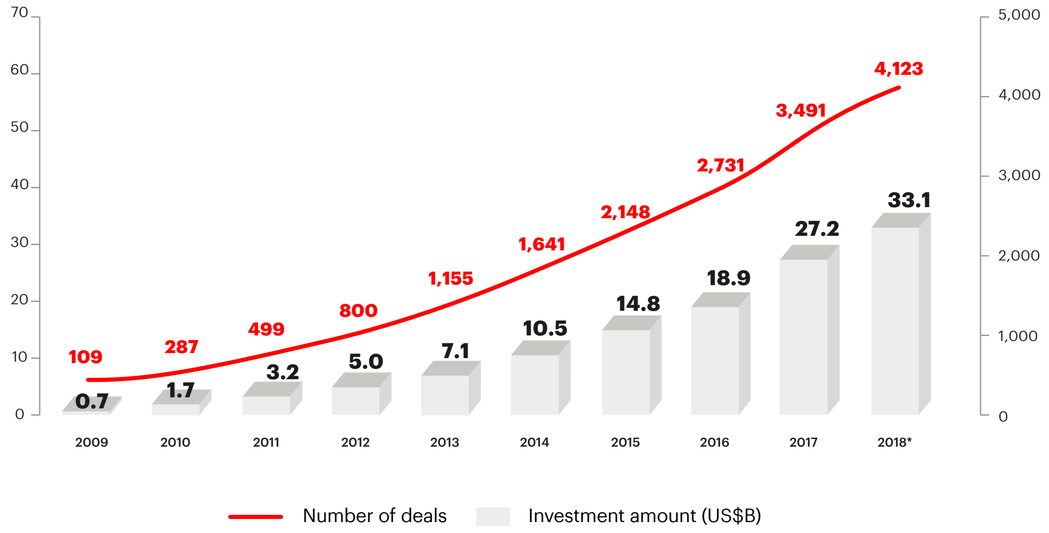
CEOs are stepping up their spending on cybersecurity to protect their businesses. In its latest security forecast, Gartner projects that such spending was more than US$123 billion for 2018 and will grow by 10.8 percent per year to nearly US$170.5 billion by 2022.[12]

The rising Internet security market is also a hot area for venture capital investors, attracting almost US$33 billion to 2,479 security startups since 2009, exceeding investments in blockchain, which have surged with the interest in business applications and cryptocurrencies. *(See Exhibit 5).*[13]

Will spending more on cybersecurity lead to a secure digital economy? In our survey, 59 percent of organizations say the Internet is becoming increasingly unstable from a cybersecurity standpoint and they are not sure how to react. While some companies aren't spending enough, others may be spending excessively in response to their low tolerance for cybersecurity risk. Others spend in the wrong areas, including projects that do not deliver effective risk reduction.

Increasing a company's cybersecurity budget may not be the answer, according to 61 percent of CEOs who believe that the security issues of the digital economy are far too big for their organization to handle alone. And 86 percent believe that taking business resiliency to the next level requires an ambitious new vision for the Internet.

Exhibit 5: Venture Capital Investments in Cybersecurity (Cumulative Data)



* As of November 2018

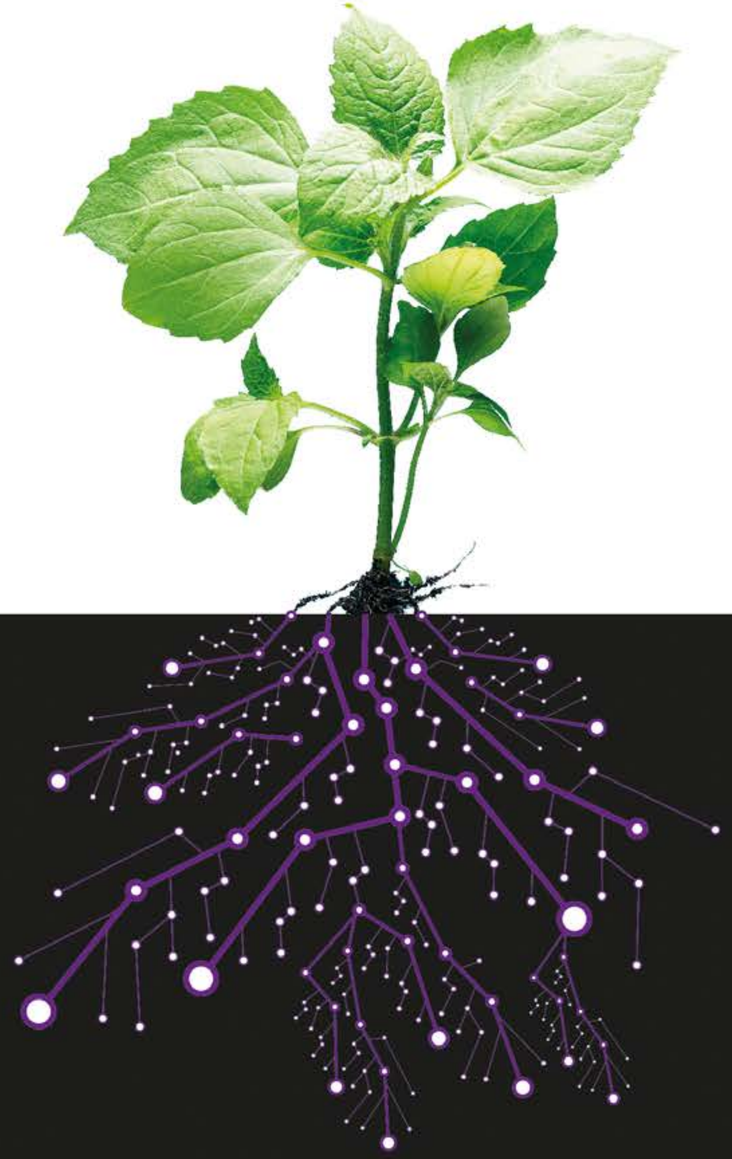
Note: CB Insights defines cybersecurity as tech-enabled companies that offer products and services for which the primary use case is the protection of digital and physical assets from unauthorized access and malicious use by cybercriminals.

Source: Accenture Research Analysis on CB Insights Data

STEPPING UP TO MAKE A STAND

How CEOs Can Help Create Digitally Secure Business Models

The oil and gas industry analogy helps reveal the types of actions CEOs can take to address security issues. In the same way that oil executives divide their focus between engineering and technological innovations below ground to advance oil and gas drilling, and above ground to develop appropriate business strategies, CEOs need a two-pronged view of the Internet security issue.



ABOVE GROUND

Leaders can do their part to build a secure Internet through industry-wide standards and best practices. CEOs can step up their governance efforts, forging collaborative relationships with peers, government representatives, regulators and industry association leads. Leaders can also embed the idea of a trustworthy digital economy in the vision for their company's business architecture, ensuring that security is prioritized within the boundaries of their company and throughout its ecosystem of partners, suppliers and end users.

To secure a trustworthy digital economy, above ground is where CEOs can own and drive the issue through business initiatives, including decisions affecting business models and ecosystems.

BELOW GROUND

Technology investments—in everything from devices to cables and networks—present decision-makers both inside and outside companies that control Internet functionality with the opportunity to build a more trustworthy digital economy. CEOs can influence and inspire technology investments that improve Internet infrastructure, but CEOs of some technology companies are in the position to apply specific technological solutions. CEOs that pay to use the Internet as a utility can understand the vulnerabilities from new technologies and influence how the Internet service is delivered securely to them. For example, they can influence investments to update the Internet's basic protocols and networks. Meanwhile, CEOs leading companies that build and own the infrastructure and equipment can ensure their products and services are equipped to handle digital business growth and can address the vulnerabilities that new technologies introduce.

ABOVE GROUND: BUSINESS INITIATIVES

Governance

Join Forces with Other Companies and Govern Globally

First, CEOs can take the lead above ground in Internet governance. Of our C-level respondents, 90 percent agree that more secure transactions will not only benefit businesses, but also consumers, government and other stakeholders.

It's in the enlightened self-interest of large businesses to extend themselves to help build a secure Internet.

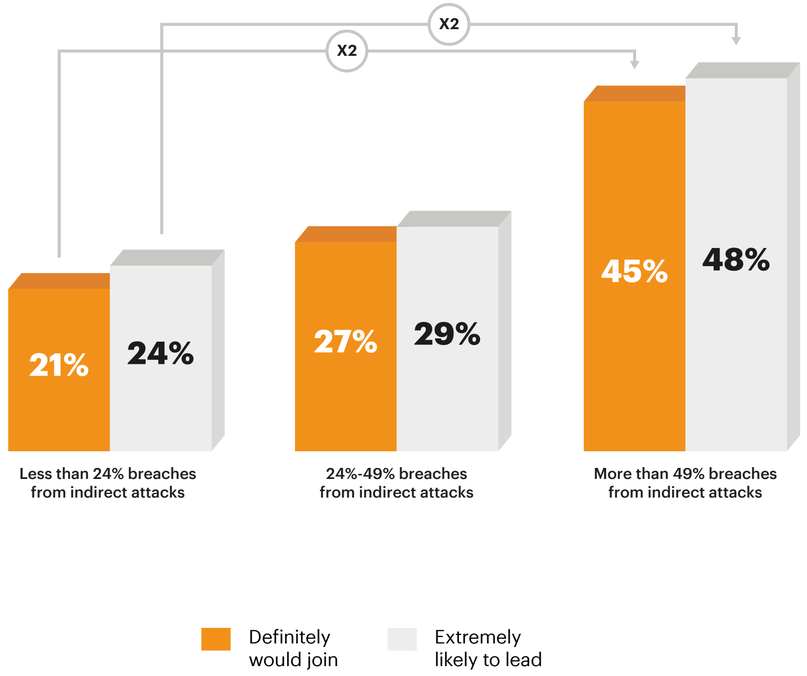
To do so, CEOs should collaborate with other top executives and also, where possible, with governments and regulators.

One venue already dedicated to this goal is the World Economic Forum's Centre for Cybersecurity. Launched in 2018, the Centre seeks to bring partners from "business, government, international organizations, academia and civil society to enhance and consolidate international security."[14]

Many companies are discovering firsthand that they can't address Internet security alone. Our survey found companies that have experienced 50 percent or more of their breaches from indirect attacks—targeted at their organization but initiated through partner organizations—are more likely to join or lead efforts to ensure the trustworthiness of the Internet economy. *(See Exhibit 6).*

But no organization should need a "wake-up call" to join an effort that results in effective guidelines and standards and influences the development of smart regulations. When leaders realize that prioritizing a trustworthy digital economy is a win-win situation, businesses, consumers and governments will all benefit through collaboration.

Exhibit 6: Likelihood to Join or Lead an Organized Effort to Govern a Trustworthy Internet Economy



Source: Accenture Research

Create an Internet Security Code of Ethical Conduct for Each Industry

A vulnerability in a pacemaker or in an avionic system can have serious consequences. Yet the software professionals who develop them are not required to attain professionally recognized accreditations similar, for example, to those required of surgeons or pilots. Code safety, ethics standards and certifications are overdue.

The creation and maintenance of a trustworthy Internet will require a formal educational system, through which software designers, solution architects, computer engineers and code developers can stay abreast of their evolving responsibilities.

As a first step to that end above ground, CEOs should promote the need for ethical codes of conduct for software professionals for their industry.

86%

of our respondents believe that in the next three years organizations in the same industry will work together more to improve resilience for their sector.

Be Proactive with Principle-based Standards

CEOs should not wait for another source to produce an ethical guide or related, principle-based standards. Choosing to proactively propose their own business-relevant, principle-based standards is a more expeditious path.

CEO guidance can, in fact, influence regulators to put in place standards that can apply to existing and future technologies instead of myriad detailed rules specific to each new technology development. For example, two-factor authentication to access banking services was already the industry standard in several markets before European regulators required it.

CEOs—especially those of device manufacturers, digital platforms and software and telecommunication providers—are uniquely positioned for this more business-friendly approach and have a responsibility to discuss design security standards for the following:

- **Devices** to ensure product transparency, the ability to make software updates and successful pre-release testing and basic offline functionalities.
- **Data** to limit unnecessary data collection or usage,[15] anonymize data, enable users to control their data and make it clear to customers that their data is being stored and used responsibly.[16]
- **Algorithms** to ensure transparency, auditability and fairness.[17]
- **Networks** to help ensure secure connection to consumers, help them in device configuration and inform them about infrastructure infections.
- **Protocols** to provide authentic routing information and reduce domain name hijacking.

Promote Consumer Control of Digital Identities

Advocating for individual control of data is more than a good public relations move. Of our C-level respondents, 86 percent say that their organization's access to digital identities is important to its ability to offer innovative customer solutions. And 87 percent of C-level respondents recognize that customers should have the right to decide how to help secure their digital identities. Maintaining the trust of customers and protecting their digital identities is paramount to the growth of the digital economy.

CEOs can't afford to stay out of above-ground debates that are already starting to take place. Regulators are discussing how countries and regions must protect people's digital identities and users themselves are becoming increasingly concerned about their online privacy. In the United States and Europe, lawmakers have already proposed or enacted regulations over consumer data privacy and Internet security.

There are two models of digital identity that CEOs should consider as influential in the discussion. In a centralized system, a single organization establishes and manages the identity system. For example, with Estonia's e-identity system, citizens are able to provide digital signatures and access a range of services using their ID cards (which have encrypted chips), Mobile-IDs (in which people use a phone) or Smart-IDs (which require only an Internet connection, no SIM card). As the Estonia example demonstrates, centralized systems can be built with specific purposes in mind to give controlling organizations such as governments the ability to vet identity data.

The alternative model is decentralized and requires the contribution of multiple entities. Its governance is more challenging unless clear rules are in place and identity can be ascertained—for example, by using blockchain technology.

As the World Economic Forum noted in a September 2018 study,[18] whatever model prevails, digital identities are deeply embedded in daily activities, leading to greater complexity and responsibility. One thing is clear: There will be mounting pressure for control over personal identity data to gravitate toward individual users. Educating customers and the general public about how to protect and use personal information shouldn't be overlooked. Being a champion of privacy and responsible management of digital identity combines sound business and corporate citizenship practices.

Commit to Sharing Information About Cyberattacks; Help Reduce the Stigma

With the heightened scrutiny on the response to cyberattacks—whether they are far-reaching or not—in the long run, transparency will build trust with everyone from suppliers to customers.

Otherwise, businesses run the risk of encountering "trust incidents," which the Accenture Strategy Competitive Agility Index shows can have a negative effect on the bottom line.[19]

To reduce the stigma from encountering these trust incidents, leaders can commit to sharing information about successful attacks and breaches.

When a company is willing to acknowledge an attack, it paves the way for more transparent work with other organizations and experts, improving their ability to resist new attacks and boosting data reliability.

Consider this:

In 2018, UK-based BT created an online portal, the Malware Information Sharing Platform (MISP), to share information about malicious websites and software with other Internet service providers—a pioneering move for a telecommunications major. It went on to sign a deal with Europol to share knowledge about cyberthreats and attacks.[20]

Of our survey respondents,

85%

already keep a careful eye on the latest security issues emerging in the Internet economy. Increased transparency will make those efforts more valuable.

Business Architecture

Connect and Protect with a Business Model That Runs on Digital Trust

To decrease the likelihood that security measures can be compromised, CEOs can make the concept of a trusted digital economy an explicit part of their organization's business model. That commitment to make security a foundational requirement should also reach through the company's entire value chain—to every partner, supplier and customer. It takes just one click to court disaster, and that click can occur inside or outside the company's walls. That's why companies need multiple layers of control to create a system that runs on digital trust, where access is given only to people who need it, wherever they are.

To ensure a trustworthy digital economy, CEOs can embed security into their business architecture—their company's business model and value chain, including their leadership structure.

As Michael Hermus, founder and CEO of Revolution Four Group and former CTO of the United States Department of Homeland Security, told us regarding the vigilance that CEOs should embed throughout a company, "You don't necessarily trust something because it looks friendly, but you really need to know exactly what it is, who it is and where it's coming from."

The first steps toward a model that ensures this trust occur within the boundaries of the organization. These steps cover the basics—security's low-hanging fruit *(as detailed in the appendix, Become Brilliant at the Basics)*.

They should be considered essential, as internal staff—either by mistake or with malicious intent—account for a sizable share of breaches. But they're also insufficient on their own. Alone, they are not nearly an adequate defense in the age of mobility and cloud technologies. That's why it is also important to take additional measures, including articulating a security by design vision, holding line of business leaders accountable for security, bringing CISOs to the board and closing off areas of exposure throughout the company's value chain.

Prioritize Security By Design

Security can't be an "add-on" feature for products and services. Instead, CEOs should articulate a vision of "security by design" from the earliest stages of development, even in the face of pressure for short-term performance.

This requires additional investment at each stage of development, but these costs often pale in comparison next to the cost of fines, recalls, lawsuits and loss of consumer confidence that companies will eventually face if they don't embrace security by design.

Although it may seem like a drastic step, CEOs who take this path probably won't be alone.

In fact, 83 percent of our survey respondents agreed that organizations must recognize the trade-off between time to market and ensuring secure, sustainable growth through technology—and always choose secure growth.

Make Line of Business Leaders Accountable for Security

Adjusting a company's remuneration system can underscore the urgency of cybersecurity concerns to leaders who are frequently rewarded for short-term financial results.

Companies can align the individual, short-term incentives of business line managers to the longer-term cybersecurity interests of the company.

One major multinational bank has strengthened cybersecurity by including the company's long-term cybersecurity interest as a factor for calculating the bonuses of the leaders of all lines of business.

Bring a CISO to the Board

About two decades ago, as the IT department left the back office to establish itself as the nervous system of a business, chief information officers (CIOs) started to appear on corporate boards.

Likewise, chief information security officers (CISOs) today can follow a similar evolutionary path.

Their area of responsibility has become too important to be confined to a single department or buried deep in the CIO organization.

One United States bank has already elevated a retired CISO to the board, forging a path for others to follow.

Managing cybersecurity doesn't mean simply avoiding software problems. It means ensuring the resilience of the entire business.

Recruiting a CISO or former CISO to the board provides the opportunity to educate fellow board members, helping them become more cyber-savvy and better risk managers.

The CISO would gain a deeper perspective on the organization. As a result, the CISO could increasingly articulate how cyber risks intertwine with other risks and inform leaders' strategic decisions.

Protect the Entire Value Chain

Based on our analysis, we estimate that if all companies collaborate to impose high standards on partner organizations, businesses can expect to save up to US$2.6 trillion.

This means that CEOs should ensure that their vision is taken into account in each interaction their company has with suppliers, clients and all other parties in their value chain. In practice, this should translate into a constant vigilance with the trustworthiness of each of the company's connections.

John Clark, professor of computer and information systems at the University of York, explained the domino effect of a lack of trust in one sector on another. "It just contributes to the denigration of trust overall rather than just in a specific application or location," Clark said.

Just as CEOs can take tangible measures to limit the far-reaching effects of cyberattacks in their ecosystem, they have other key opportunities to protect trust for the digital economy as a whole.

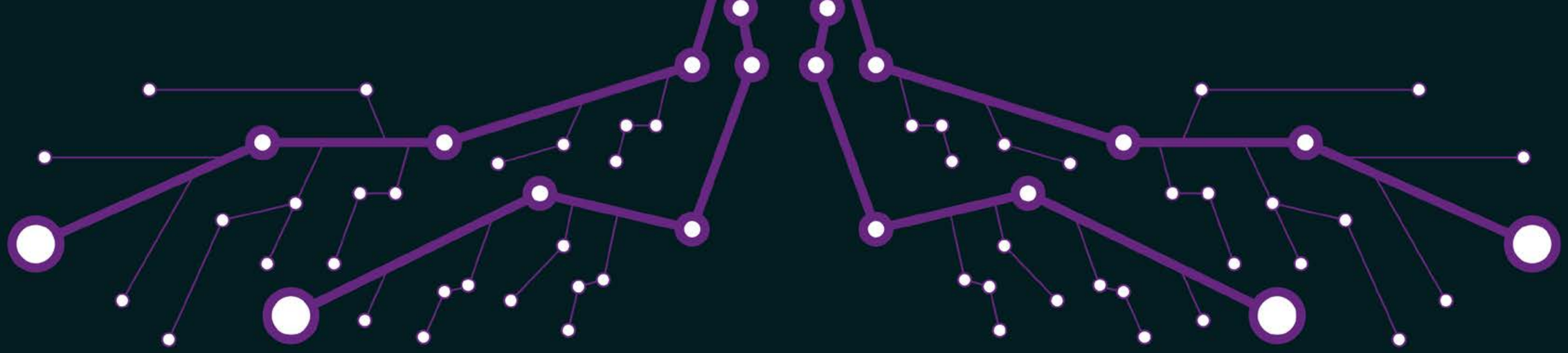
Of the corporate leaders surveyed,

82%

agree that it is the responsibility of large organizations to foster a digital ecosystem that includes small and medium businesses to help them operate in a trustworthy digital environment in the interests of all.

62%

note that it is difficult to control indirect cyberattacks that are targeted at their organization but initiated through partner organizations.



BELOW GROUND: INTERNET INFRASTRUCTURE

Technology

Advance Businesses and Enhance Safety Through Technology

Inside and outside the technology sector, all CEOs have a role to play when it comes to the technology for a secure Internet.

The CEOs who oversee technologies powering and protecting the Internet can deliver solutions securely below ground—for the Internet's basic protocols, devices, advanced networking and computing.

But all CEOs can ensure the growth of the digital economy by demanding a safer, more crime-resistant Internet for their business.

Chuck Robbins, CEO of Cisco, addressed this opportunity in his remarks at a recent World Economic Forum event.

As tech leaders, we have to step up and get in the middle of these issues. We cannot wait for governments to solve them. Companies who compete with each other need to put that aside to bring our experience together to help us get at this problem."

Chuck Robbins, CEO, Cisco[21]

Resolve Vulnerabilities in Basic Internet Protocols

Realizing long ago that the main line of defense against cybersecurity doesn't take place at the end points (personal computers, mobile phones and IoT devices), the technology community has proposed solutions to add security to the base Internet protocols.

For example, to solve the vulnerabilities of the Domain Name System (DNS), a technology called DNS Security Extensions (DNSSEC) digitally "signs" data so a user knows it's valid.

Because this is a highly technical issue, the biggest impact of the majority of CEOs will be to influence Internet service providers—and others who manage hardware—to upgrade systems against vulnerabilities.

As the IoT age continues to proliferate end points, the Internet will require an alternative to Transmission Control Protocol (TCP)—a system that sends data packets over networks on the Internet—to support offline sessions and provide a secure alternative for multiple devices that were previously sharing an IP address.

Investments in new protocols produce benefits only if enough networks choose to invest.

CEOs are in a position to influence Internet service providers as a first action to make the Internet more secure and to invest in implementing better base Internet protocols. The leverage of a CEO to influence below-ground activities should not be underestimated.

Heighten Security at the Edge

The edge computing universe—including servers, mobile phones, IoT devices—represents a revolutionary stage of the Internet to analyze data in real time.

Instead of sending data across long routes and processing it in a centralized data center or the Cloud, it's processed near the edge of a computer network where data is generated.

But the variety of devices computing at the edge means security practices are inconsistent across technologies. Indeed, 86 percent of our respondents agree that security needs to be embedded into technology, particularly with regard to the IoT and Industrial IoT (IIoT).

Software development life cycles, including those developed by the National Institute of Standards and Technology (NIST), are being modified to ensure that software security and update functions are embedded from the beginning.

Following a 2016 vulnerability in Tesla's WiFi and onboard entertainment system, Tesla not only patched the bug via over-the-air updates but also implemented a code-signing policy under which all firmware in cars needs to be validated and verified.

Today, Tesla implements dozens of safety and security measures annually; its cars do not carry model years, reflecting the idea that cars are evolving into devices that can be improved regularly.[22]

As the example of Tesla demonstrates, technology CEOs can make greater use of network architectures to more quickly detect and mitigate edge-related threats.

Through collaborative work with cross-industry coalitions, they can develop standards for edge devices, establish certification frameworks similar to international mobile phone standards and incentivize the ongoing adoption and evolution of security innovation.

Embrace the Advantages of Software-Defined Networking

Software-Defined Networking (SDN) is a maturing architecture that creates dynamic network environments that exist for the limited time required to complete specific tasks.

Its short-lived nature makes network end points difficult to identify and the network pathways harder to find and attack than those of traditional fixed network solutions.

SDN improves network control by enabling Internet service providers and other businesses to respond quickly and cost-effectively to high-bandwidth demands. It also automatically enables "ring-fenced" data centers if it detects malicious activities, limiting the chance of contagion.

While some CEOs may be deterred by the cost of deploying SDN, those of large companies could have the resources to contribute to this technology. Others can "inspire and influence" its development for the benefit of all.

Tackle the Question of Quantum

No longer science fiction, quantum computing exploits the laws of quantum mechanics to process information with quantum bits, or qubits, instead of manipulating long strings of bits encoded as a zero or one. Opportunity areas for quantum computing could be in fraud detection for financial services, supply chain and purchasing, advertising scheduling and advertising revenue maximization for the media industry.[23]

There is no agreement about when a quantum computer that surpasses the capacity of a traditional computer will be available, but two things are clear. First, quantum computers will provide a significant boost to the world's computing power. Second, they will be able to more easily break most current encryption methods.

These points generate much uncertainty about the future of cybersecurity. The most productive course for CEOs is to move ahead with current security activities and stay informed of the evolution of quantum computing. In practice, leaders can position themselves for quantum-resistant encryption by appointing a working team of "quantum monitors" to identify where the technology is most likely to impact their business security. Accessing emerging application programming interfaces (APIs) will enable businesses to develop pilots for quantum-based optimization, sampling and machine learning. Through such pilots companies can test, learn, iterate and stand ready.

PAVING THE WAY FOR A TRUSTWORTHY DIGITAL ECONOMY

Today's security strategies are, in large part, still responding to yesterday's challenges. From reports of exposed personal information to data misuse, trust incidents are becoming increasingly visible to the public. Regaining lost trust is an uphill battle. And many CEOs aren't aware of its value until it's too late.

Our research shows businesses can quantify the impact of a trusted digital economy on the bottom line, and 90 percent of our respondents say a trustworthy digital economy is very or extremely critical to their organization's future growth.

The actions of CEOs—driving above ground and influencing below ground—matter.

By joining forces with other CEOs, public sector leaders and regulators, they can develop much-needed guidelines and oversight mechanisms.

By protecting their own organization and extending protection through its value chain, they will safeguard the business ecosystem.

By embracing and developing technologies that can advance their businesses and enhance digital safety, CEO engagement can drive a trust turnaround for the Internet and secure the future of the digital economy.

APPENDIX

Become Brilliant at the Basics

Adopting Best-in-Practice "Cyber Hygiene" Techniques Means Becoming Brilliant at the Basics, Including:

Training people

When a company starts using technology that many or even most of its relevant employees don't understand, the firm is bound to suffer from lost opportunities or higher cyber vulnerabilities—or both. Security will be determined by the company's weakest link; often that is an employee who inadvertently presents the opportunity for a breach. Yet systematic training is, in general, still not accepted as a basic practice, even with attacks increasing in frequency, size and scope. Incentives are also important: Some companies are linking executives' remunerations to security.

Protecting against phishing

Hackers often use social engineering tactics, such as phishing, to attack companies, so training to avoid falling in this trap is especially important.

Passwords

Though it sounds obvious, many companies still struggle with the implementation of cybersecurity basics, such as sound password policy. Multifactor authentication should be the default option for every business.

Patching

Unfortunately, when a company detects a vulnerability, the fix is often put off until security managers and staff "have time." Now is the time to prioritize fixing any detected weaknesses.

The Value of Cybersecurity for Businesses and Society

Many have talked about the costs of cyberattacks, but what about the other side of the coin? How might better cybersecurity practices create value for businesses and society?

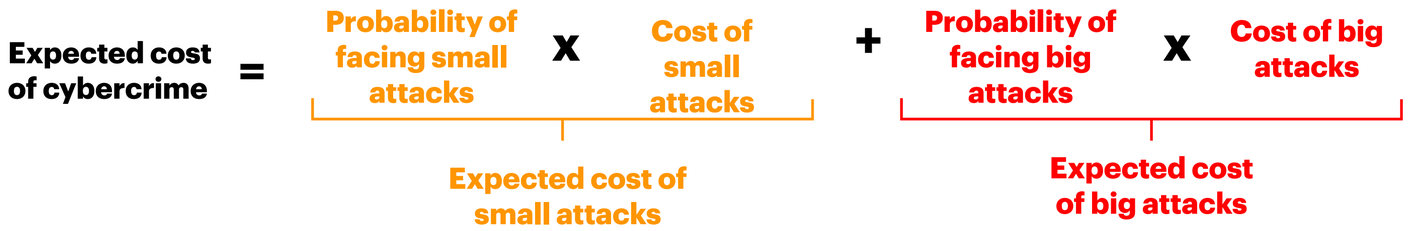
Driven by understanding both the cost of crime and the potential of a trustworthy digital economy, we conducted our analysis in three steps.

The Expected Cost of Cybercrime

We began by estimating the expected cost of cybercrime in terms of revenue for a company of a given size in a range of industries. We measured the value exposed, considering the risk of small (less than 90,000 records impacted) and big (more than 90,000 records impacted) attacks and the probability of their occurrence. Revenues by company size and industry were sourced from Capital IQ. Calculating the cost of small attacks required the following elements:

- Annual costs of cybercrime by company size and industry, sourced from Ponemon Institute data for the Accenture 2018 Cost of Cybercrime study.
- The industry average number of days it takes to fix damage caused by an attack and the average number of attacks in a year, sourced from the survey report "Gaining ground on the cyberattacker: 2018 State of Cyber Resilience."[24]

We drew the estimated cost of a big attack from our event study, described below in the section entitled "The impact on revenue of a big, public event." We sourced the probability of a big event from Ponemon Institute data for the Accenture 2018 Cost of Cybercrime study. The findings of our survey (conducted for this study) provided the portion of attacks coming through third parties.



The Value at Risk for Businesses

Next, we estimated the expected value at risk by industry. We calculated the total industry revenues and multiplied those figures by the expected cost of cybercrime.

The sample consisted of 4,700 companies. These were publicly listed companies with more than 250 employees, operating in the industries under scope and headquartered in the countries under scope.

Company revenues were sourced from Capital IQ. Revenue forecasts for the 2018 to 2023 period were obtained by extrapolating current revenues forward, according to the 2011 to 2017 CAGR from Capital IQ data.

Value at risk for businesses = **Expected cost of cybercrime** x (**Company average revenue** x **Number of companies in our sample**)

(**Company average revenue** x **Number of companies in our sample**) = **Total industry revenue pool**

The Economic Picture for a Trustworthy Internet

Finally, we analyzed how an increase in companies' cyber resilience and the trustworthiness of the Internet could translate into less value at risk for business and society. We modeled econometrically how companies' lower vulnerability, measured by the number of attacks suffered and the number of days it takes to solve an incident, reduces the cost of cybercrime after the introduction of better cybersecurity practices. We then estimated how this gain translates into value for society.

We estimated an econometric model to calculate the probability for a company of (a) receiving a certain amount of attacks and (b) solving a data breach within a certain period of time.

The data set comprised 4,500 companies in the Accenture 2018 State of Cyber Resilience survey.[25] The explanatory variables included: 1) the percentage of spend in cybersecurity over total IT spend; 2) whether companies impose high standards on business partners, and; 3) whether companies had made significant cybersecurity investments in the prior six months.

We used the estimated coefficients to recalibrate the Value at Risk Model and formulate an alternative scenario in which every company: 1) regularly (every six months) makes significant investments in cybersecurity; 2) invests as much as the top 20 percent of performers in cybersecurity; and 3) imposes high standards on business partners.

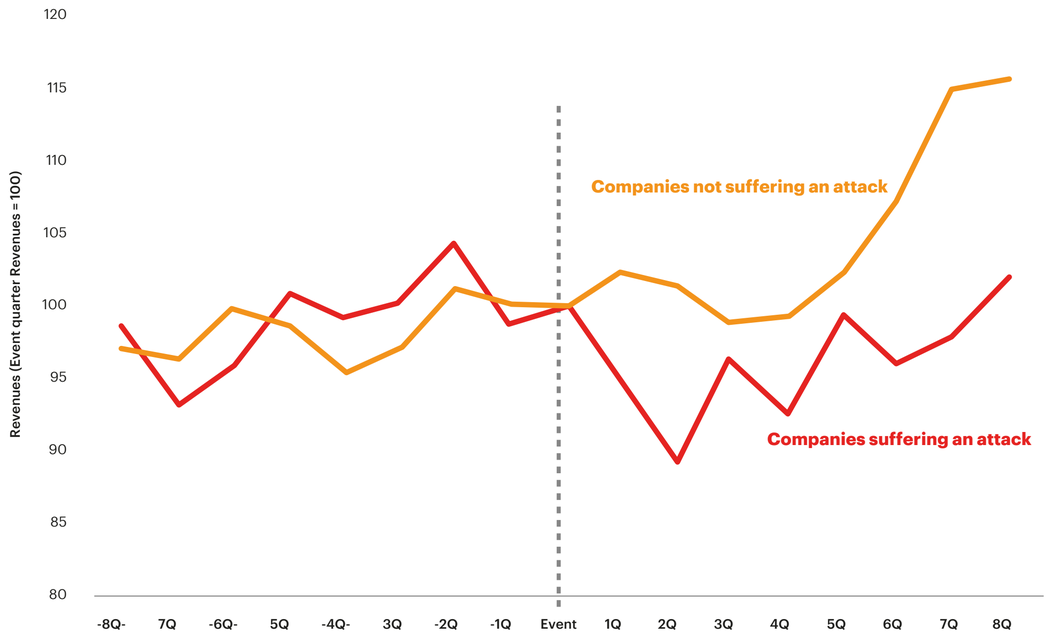
The Impact on Revenue of a Big, Public Event

We identified unique cyberattacks that were publicly announced by the companies attacked using Breachlevelindex.com by Gemalto. Breachlevelindex.com collects information of all public attacks since 2013. Each attack is assigned a risk level from 1 to 10, where events above a risk score of 5 are classified as critical to severe.

We collected all the events that had a risk score above 5, then we excluded events related to government agencies and universities. Our final sample included 460 unique events and 436 unique companies. Among them, approximately 80 are publicly traded. For these companies, we collected revenues information from S&P Capital IQ.

In the event of negative cybersecurity events, revenues experienced a decline. To identify a causal effect, we created a control group composed of the top 10 peers (as defined by S&P Capital IQ) of each breached company. Under the assumption that the control group was not breached, we used an event study methodology (diff-in-diff estimation) to compare the two sets of companies and calculate the percentage change in revenues, comparing eight quarters before and after the event.

Exhibit 7: Big and Public Cyberattack Impact on Revenue



Source: Accenture Research

Transcript Analysis

Our transcript analysis was based on transcripts of earnings calls of companies present in the S&P 500 as of October 1, 2018.

We collected 11,418 unique transcripts from S&P global, covering a time frame from September 1, 2012, to August 31, 2018.

Text data was analyzed using two different algorithms: one to identify mentions and discussion about cybersecurity; and another to calculate the intended strategy toward cybersecurity.

We identified cybersecurity mentions by checking for certain keywords (and possible combinations of those keywords) in each sentence in the transcripts. When we found a match, we marked the sentence as being cybersecurity related. We used the following keywords: cybersecurity, cyberattack, cyberthreat, cybercrime, cyber incidents, cyber intrusions, cyber theft, cyber fraud, malicious cyber activity, adverse cyber event, data leak, data breach, malware, ransomware, spyware, IP theft, DDoS attack.

Using a proprietary neural network algorithm that captures a company's attitude toward cybersecurity, we then calculated an intended strategy.

Our model uses a long short-term memory neural network (a deep learning NLP model that accounts for word order and context) to identify a company's strategic orientation and long-term focus, and the clarity of its strategic vision.

To develop our AI, 900,000 sentences were randomly selected. This set was further split into three subsets:

- a training dataset (80 percent),
- a testing dataset (15 percent) and
- a cross-validation dataset (5 percent).

Subsequently we applied the estimated model to all the sentences from our transcript dataset.

Acknowledgments

Authors

Omar Abbosh

Kelly Bissell

Research Lead

Luca Gagliardi

Project Team

Edward Blomquist

Tomas Castagnino

Francis Hintermann

Lynn LaFiandra

Ryan LaSalle

Regina Maruca

Vincenzo Palermo

Tom Parker

Eduardo Plastino

Virginia Ziegler

We would like to thank the following business leaders, experts and practitioners for their valuable insights during our interviews and conversations:

Jay Best
Crypto Strategy Advisor, Itsa Ltd.

Elaine Bucknor
CISO, Sky TV

John Clark
Professor, Computer and Information Systems University of York

Afonso Ferreira
Professor, Director of Research, CNRS - Toulouse Institute of Computer Science Research

Norman Frankel
Chairman, iCyber-Security

Per Gustavson
Information Security Expert, GDPR, Göteborgs Stad

Jeff Hancock
Co-Founder and Chief Operations Officer, getFIFO

Muhittin Hasancioglu
Former VP and CISO, Royal Dutch Shell plc

Michael Hermus
CEO & Managing Partner, Revolution Four Group, LLC

Naoki Kamimaeda
Investor, Mad Street Den

Arthur Keleti
IT Securities Strategist, T-Systems

JJ Markee
CISO, KraftKeinz

Amit Mital
CEO at Kernel Labs Holding Llc, Former CTO Symantec Corporation

Peter Morgan
Founder and CEO at Deep Learning Partnership

Tony Sager
Senior Vice President and Chief Evangelist, CIS (Center for Internet Security)

Adam Segal
Director of the Digital and Cyberspace Policy Program; Council on Foreign Relations

PW Singer
Senior Strategist; New America

George Smirnoff
CISO, Synchrony

John Valente
CISO, The 3M Company

Uwe Wirtz
CISO, Henkel

Sources

1 https://www.Internetworldstats.com/emarketing.htm

2 *Gartner, Forecast Analysis: Internet of Things—Endpoints, Worldwide,* 2017 Update

3 https://www.ericsson.com/en/mobility-report/reports/november-2018/network-coverage

4 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

5 https://www.zdnet.com/article/this-is-how-much-the-wannacry-ransomware-attack-cost-the-nhs/

https://www.bbc.com/news/health-39899646

6 *Dow Jones Factiva and Accenture Research analyses*

7 https://bgpmon.net/popular-destinations-rerouted-to-russia/

8 https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/?noredirect=on

9 https://www.avatier.com/blog/how-single-sign-on-works/

10 *Accenture Research analysis on Facebook Annual Reports*

11 *Accenture Research analysis on ITI and Oxford Economics data*

12 *Gartner, Information Security, Worldwide,* 2018 Update, October 5, 2018

13 *Accenture Research analysis on CB Insights data*

14 https://www.weforum.org/centre-for-cybersecurity

15 *Fjord Trends 2019, a report that examines seven trends shaping business, technology, and design. One of the seven: Data Minimalism.* For more information, see: https://www.fjordnet.com/conversations/fjord-launches-2019-trends-report/

16 Note: Europe is at the forefront of the change toward more secure, trustworthy digital ecosystems. Its General Data Protection Regulation (GDPR), which came into force last year, gives organizations 72 hours after identifying a data breach that could "result in risk for the rights and freedoms of individuals" to report it to their supervisory authority. Moreover, organizations in breach of GDPR—for example, not having strong enough customer consent to process their data—can be fined 20 million euros or up to 4 percent of their annual global turnover, whichever is greater. Pressure on businesses is mounting. The UK Information Commissioner's Office (ICO), for example, received 6,281 data protection complaints between May 25, 2018 (when the new regulation came into force) and July 3, up from 2,417 in the same period the previous year. (https://eugdpr.org/ and https://edexec.co.uk/gdpr-compliance-is-a-journey-not-a-destination)

17 *"Auditing Algorithms for Bias", Rumman Chowdhury and Narendra Mulani, HBR* October 2018

18 *World Economic Forum, "Identity in a Digital World – A new chapter in the social contract",* September 2018.

19 *Accenture, The Bottom Line on Trust,* November 2018 https://www.accenture.com/us-en/insight-competitive-agility-index

20 https://securitybrief.eu/story/bt-and-europol-join-forces-stem-global-cybercrime-epidemic/

21 *WEF: Creating a Shared Future in a Digital World,* https://www.youtube.com/watch?v=C7mfNNfDpec

22 https://www.wired.com/2016/09/tesla-responds-chinese-hack-major-security-upgrade/

23 *Accenture, 2018 State of Cyber Resilience, April 2018* https://www.accenture.com/us-en/insights/security/2018-state-of-cyber-resilience-index

24 "*Quantum Computing: From Theoretical to Tangible", Accenture* 2018. https://www.wired.com/2016/09/tesla-responds-chinese-hack-major-security-upgrade/

25 *Accenture "Gaining ground on the cyber attacker 2018 State of Cyber Resilience"* 2018 https://www.accenture.com/us-en/insights/security/2018-state-of-cyber-resilience-index

About the Authors

Omar Abbosh

Group Chief Executive, Accenture Communications, Media & Technology

omar.abbosh@accenture.com

Omar is responsible for the company's US$8 billion business serving the digital platforms, media, telecommunications, semiconductor and consumer electronics industries.

Before being appointed to his current position, Omar served as Accenture Chief Strategy Officer where he orchestrated the organization's digital transformation, pivoting the company's core business to Digital, Cloud and Security services, which now account for 60 percent of revenues. He successfully launched and scaled new businesses such as Accenture Security, and built Accenture Innovation Architecture, including its flagship Innovation Hub in Dublin. His experience and deep connections in Silicon Valley allow him to stay ahead of key shifts across multiple technologies.

Omar is a member of the Accenture Global Management Committee. Before being appointed to his current position in September 2018, he served as Accenture Chief Strategy Officer for more than three years, with responsibility for overseeing all aspects of the company's strategy, strategy implementation, innovation programs and investments. This included ventures and acquisitions, The Dock—the Accenture flagship innovation facility—industry programs and Accenture security business.

Omar brings three decades of experience to his role. Previously, he held several management roles including senior managing director, Growth & Strategy for the Resources operating group. He has served as the global client lead for leading multinational companies where he advised client executives on major strategic issues for their businesses.

Omar holds a degree in Electronic Engineering from Cambridge University and a Master's Degree in Business Administration from INSEAD.

Kelly Bissell

Senior Managing Director,
Accenture Security

kelly.bissell@accenture.com

Kelly leads the company's US$2 billion security business across all industries. In this role, he spearheads the organization's commitment to help clients build cyber resilience and grow with confidence in a landscape of increasing range of threats.

Kelly has spent more than 30 years bringing innovative, strategic solutions to help global organizations address a range of complex security challenges. As a recognized cybersecurity expert, Kelly specializes in incident response, identity management, privacy and data protection, secure software development, and cyber risk management. With a commitment to help clients innovate—safely and securely—Kelly has a vision to help businesses embed security in everything they do.

Previously, Kelly held various leadership positions with Arthur Andersen, BellSouth (AT&T), Deloitte & Touche LLP, Medaphis, and McKesson. During his career, he has served in almost every IT capacity from developer, network engineer, data center director, CISO, CTO and CIO.

Kelly received a Bachelor of Science in Computer Information Systems and earned a Master of Business Administration from Emory University.

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 469,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives.

Visit us at www.accenture.com

About Accenture Strategy

Accenture Strategy combines deep industry expertise, advanced analytics capabilities and human-led design methodologies that enable clients to act with speed and confidence. By identifying clear, actionable paths to accelerate competitive agility, Accenture Strategy helps leaders in the C-suite envision and execute strategies that drive growth in the face of digital transformation.

For more information, follow

@AccentureStrat

or visit

www.accenture.com/strategy

About Accenture Research

Accenture Research shapes trends and creates data driven insights about the most pressing issues global organizations face. Combining the power of innovative research techniques with a deep understanding of our clients' industries, our team of 300 researchers and analysts spans 20 countries and publishes hundreds of reports, articles and points of view every year. Our thought-provoking research—supported by proprietary data and partnerships with leading organizations, such as MIT and Harvard—guides our innovations and allows us to transform theories and fresh ideas into real-world solutions for our clients.

For more information, visit

www.accenture.com/research