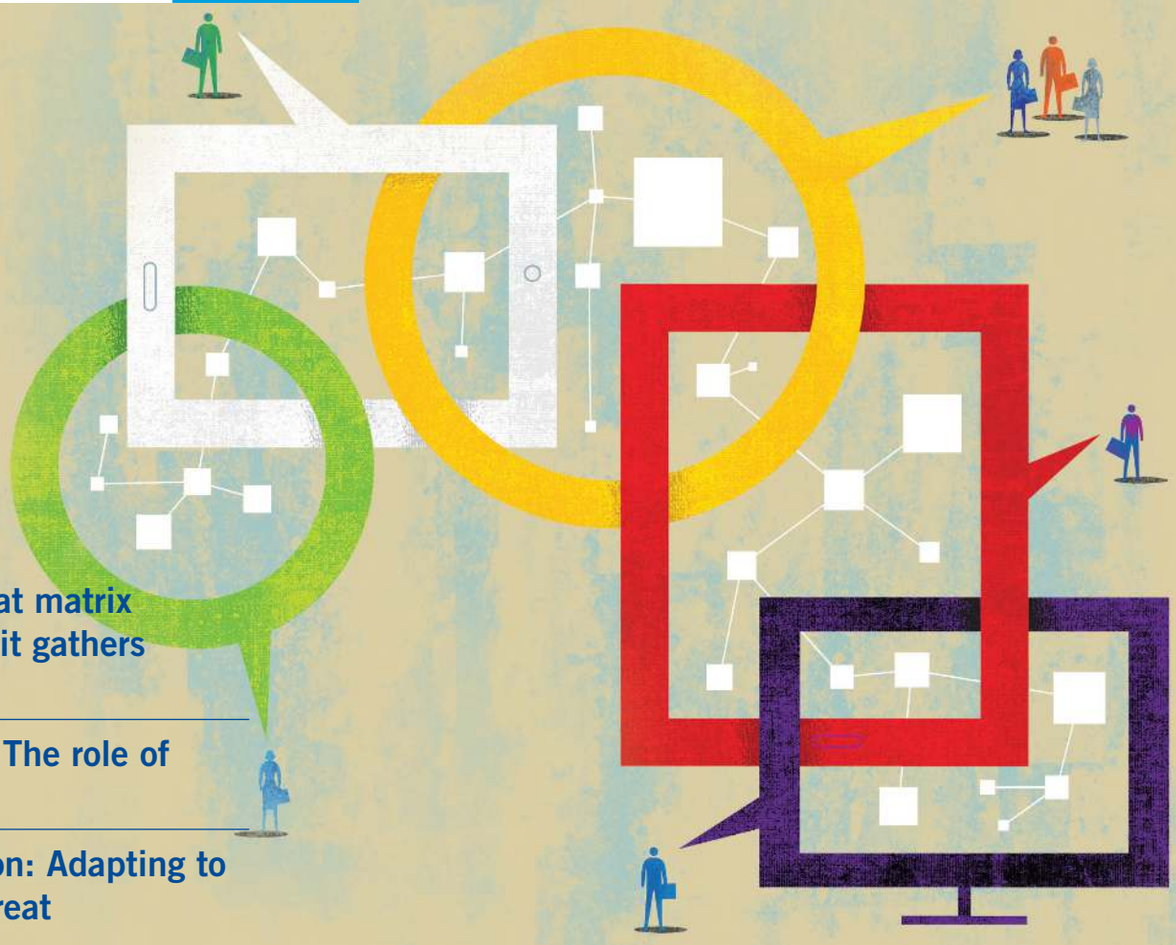
Cybersecurity: Trade-offs in technology

FRANKLIN TEMPLETON THINKS™ DISRUPTION



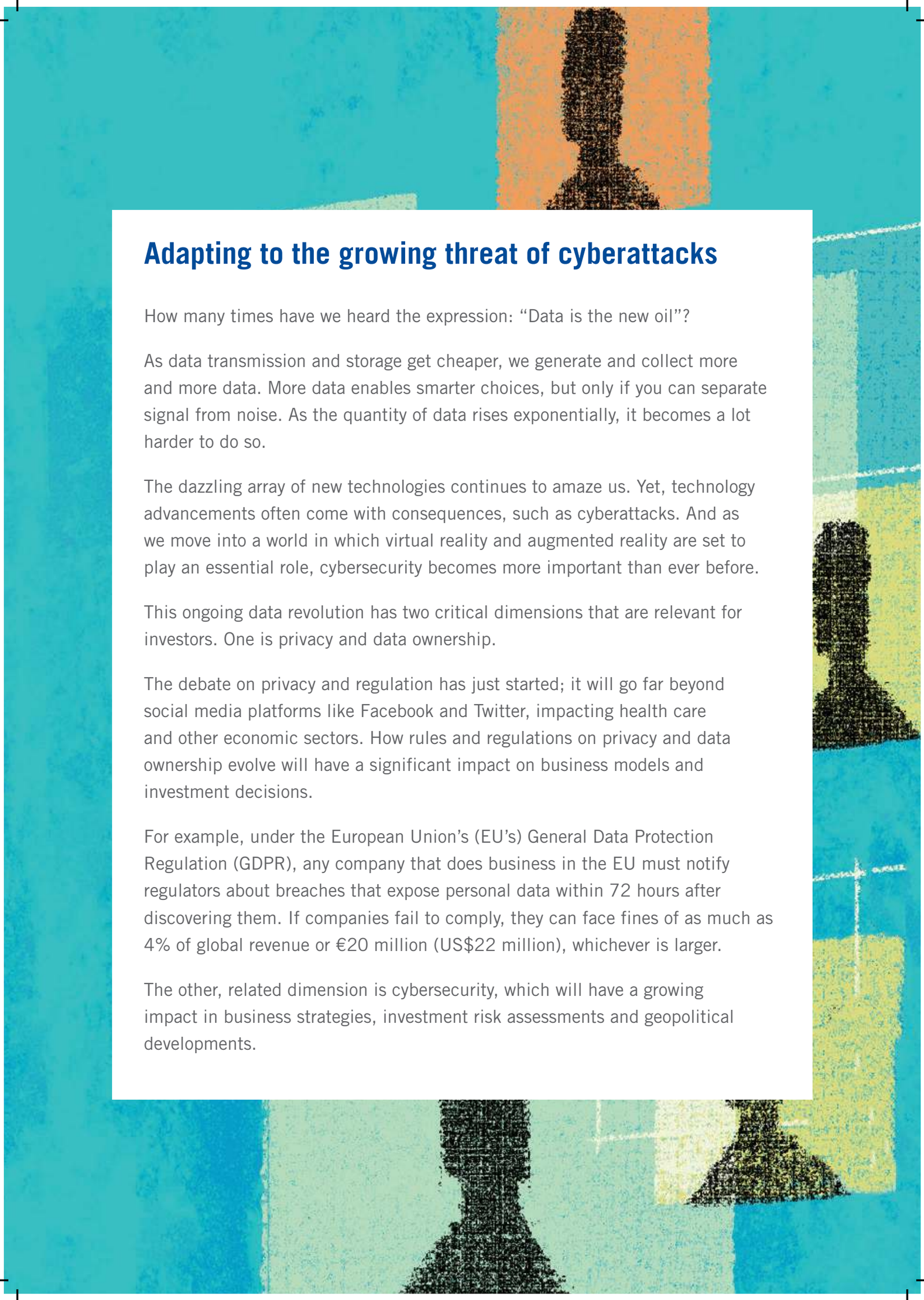
OCTOBER 2019

The cyber threat matrix accelerates as it gathers sophistication

Fighting back: The role of cybersecurity

Cyber escalation: Adapting to the growing threat

FRANKLIN TEMPLETON



Adapting to the growing threat of cyberattacks

How many times have we heard the expression: “Data is the new oil”?

As data transmission and storage get cheaper, we generate and collect more and more data. More data enables smarter choices, but only if you can separate signal from noise. As the quantity of data rises exponentially, it becomes a lot harder to do so.

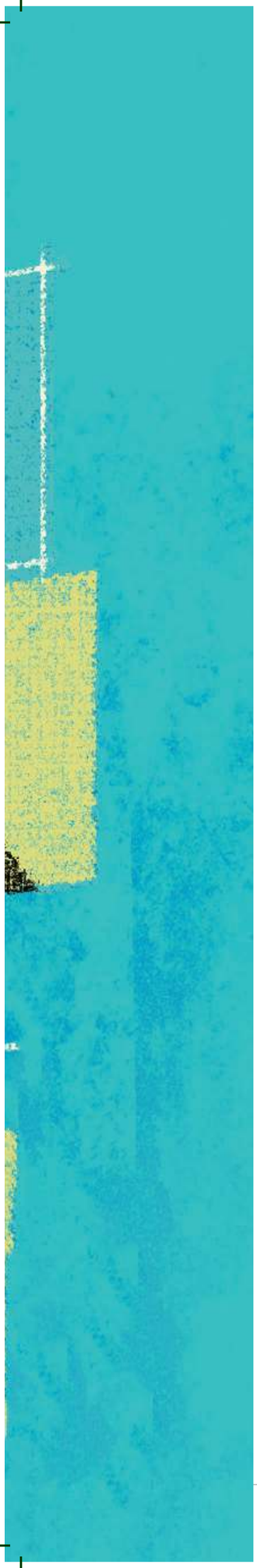
The dazzling array of new technologies continues to amaze us. Yet, technology advancements often come with consequences, such as cyberattacks. And as we move into a world in which virtual reality and augmented reality are set to play an essential role, cybersecurity becomes more important than ever before.

This ongoing data revolution has two critical dimensions that are relevant for investors. One is privacy and data ownership.

The debate on privacy and regulation has just started; it will go far beyond social media platforms like Facebook and Twitter, impacting health care and other economic sectors. How rules and regulations on privacy and data ownership evolve will have a significant impact on business models and investment decisions.

For example, under the European Union’s (EU’s) General Data Protection Regulation (GDPR), any company that does business in the EU must notify regulators about breaches that expose personal data within 72 hours after discovering them. If companies fail to comply, they can face fines of as much as 4% of global revenue or €20 million (US$22 million), whichever is larger.

The other, related dimension is cybersecurity, which will have a growing impact in business strategies, investment risk assessments and geopolitical developments.



Key takeaways

1. The sophistication and scope of cyberattacks continue to rise. Convenience for consumers may be offset by disruptions to industries and to productivity.

2. Marrying the benefits of interconnected technology with the minimization of cybersecurity threats requires carefully considered trade-offs. Sometimes the weakest link in cybersecurity is not in the software, but in its human operators.

3. We believe investors should categorize cybersecurity as an economic issue—similar to how they categorize climate change mitigation and adaption, water crises or other environmental, social or governance challenges.

4. In our view, all these issues identify additional sources of potential risks and opportunities for investments that are often lurking beneath the surface of corporate and sovereign balance sheet information alone.

The cyber threat matrix accelerates as it gathers sophistication

The connected world is a profitable playground for hackers because it is riddled with bugs. The consequences of poor security keep businesses and consumers from reaching for new technologies as they begin to question the wisdom of connecting everything.

Cybercrime—any criminal activity using a computer or other networked device to obtain valuable information and data—costs the world an estimated US$600 billion, or 0.8% of global gross domestic product (GDP), according to a 2018 report from McAfee and the Center for Strategic and International Studies.[1]

The more connected we are, the more vulnerable we are to ransomware and cyberattacks. The soft spots are multiplying, and no industry or digital gadget is immune. All internet-connected devices are potentially exposed.

>700Mil

consumer identities are stolen every single year.[2]

The list of security gaps is long. Programmers are human; even the best of them can introduce numerous coding defects despite strict supervision. As they vie for market share and tap into the consumerist desire for convenience, their infected devices can become part of a "botnet," or an army of computers in thrall to pernicious malware (malicious software).

Hackers will be keen to infiltrate the controls and data pertaining to public utilities, traffic and road conditions, even garbage collecting and the interior workings of individual homes. As cities add connectivity to their power supplies, CCTV networks, transit lines and other services, they are increasing the number of hackable targets.

A wide range of targets

On the infrastructure grid, we now have high-tech digital power plants and meters, traffic signals, semi-autonomous vehicles with web-connected sensors, pollution sensors, sewer-management systems, dams and flood-detection devices—all hackable. Even when just a single Internet of Things (IoT) sensor or government employee's computer is breached, the damage can cause a chain reaction through the system as the opportunities for hackers to inflict harm grow exponentially.

>246Mil

viruses were put into the world last year alone.[3]

TYPES OF CYBER ATTACK

State-sponsored actor attacks

US / UK / The Netherlands / Germany have publicly indicted state-actors

Large-scale data provider attacks

Cloud providers / Telecoms / Data brokers seeing elevated attack activity

Monetary extortion cases

Non-attributable currencies (e.g., Crypto) enabling anonymous ransom payments

Attack-to-detection dwell time

Average days:
78 in 2018
101 in 2017
416 in 2011[4]

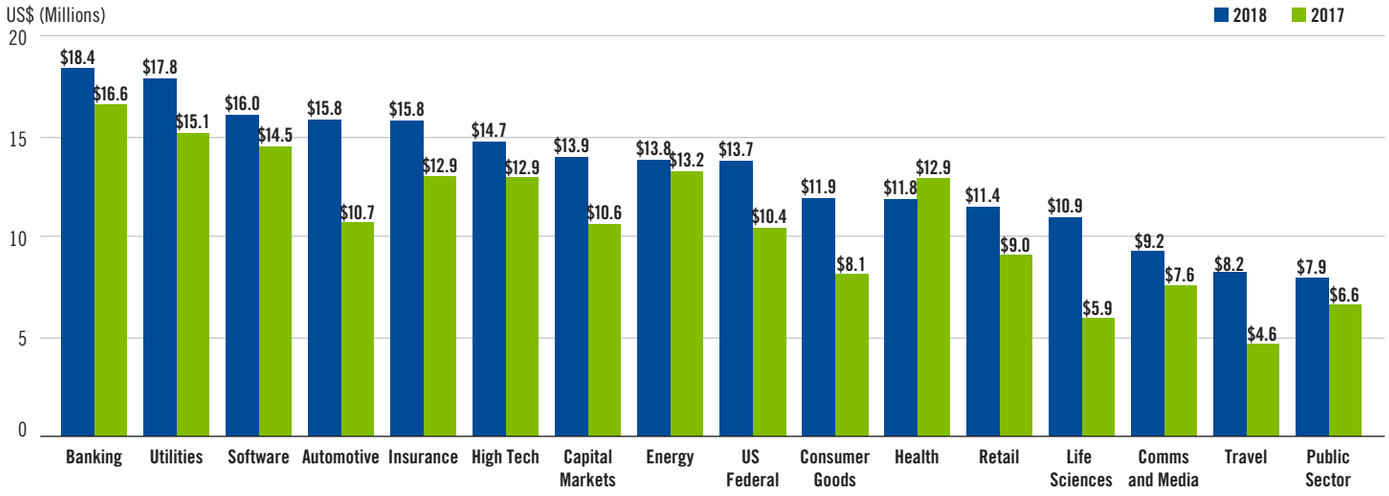
THE EXTENT OF THE CYBER THREAT

The average financial institution is typically attacked millions of times every single day, well over a billion times a year. Last year, the US Post Office was attacked four billion times. It's seen as a back door into the rest of the US government, which makes it an attractive target.

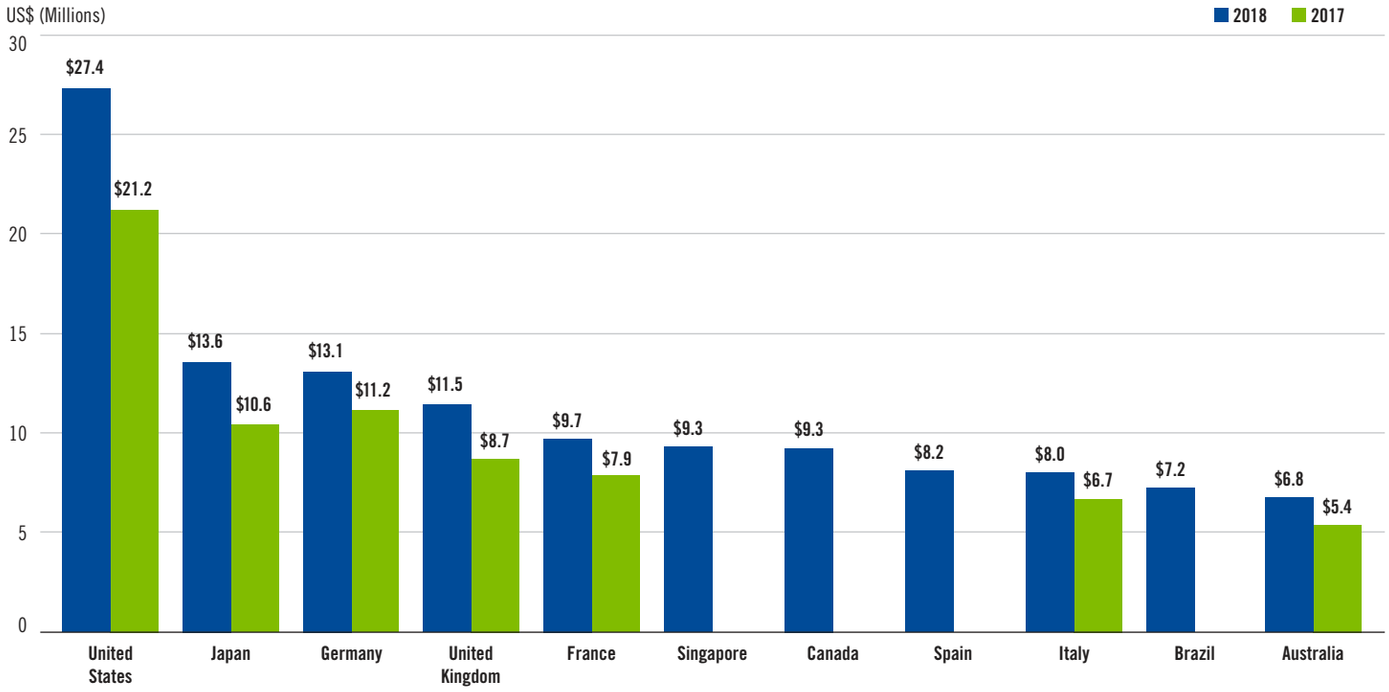
Hacktivists account for almost 85% of attacks on global companies. Around 13% of those conducting attacks are cybercriminals. They are incredibly motivated to get information and sell it on the dark web. Medical information is often viewed as the most valuable information. According to the latest analysis by Symantec, cybercriminals are successful about 15% of the time. We consider that a disconcertingly high rate.

State-sponsored attacks make up 1% to 2% of the attack vector, but are successful more than 98% of the time.

THE AVERAGE ANNUAL COST OF CYBERCRIME BY ORGANIZATION (INDUSTRIES)



THE AVERAGE ANNUAL COST OF CYBERCRIME BY ORGANIZATION (COUNTRIES)



Source: Accenture. The Cost of Cybercrime. March 2019. Based on data from 355 participating organizations.

Security researchers have also identified the ability to hack medical devices, including pacemakers and insulin pumps. In 2017, the US Food and Drug Administration issued its first cybersecurity-based recall, having discovered select wireless pacemakers exhibiting weak defenses against hackers. When manifested in telecommunications equipment, government officials fear it could be used to spy on the internet and on communications traffic that it carries.

EVERY 90 DAYS

730Mil

new websites are established, 73% of them are around for less than 24 hours.

Modern vehicles ride on millions of lines of code that have been provably hacked and manipulated from afar. Malicious software can unencrypt sensitive data and remotely sabotage complex supply chains.

Many people like to think digital currency "hot wallets"—a type of bitcoin wallet that is connected to the internet and protected by sophisticated blockchain technology and crypto-currency exchanges—can't be compromised. However, they may now be imbued with a fading, false sense of security as new tools are created to circumvent their user application programming interface (API) keys and two-factor authentication (2FA) codes.

CRYPTOCURRENCIES HAVE REVOLUTIONIZED HACKING AND CYBERSECURITY

It used to be difficult to steal a hundred million dollars. A determined hacker might have been able to siphon off $10,000, or $20,000 there, but getting a very large sum of money out of the financial system was more complicated.

There have been some high-profile examples of criminals successfully scamming several million dollars. However, they were caught and jailed before being able to benefit from their crimes because the money was still trapped in bank accounts overseen by a tight web on multinational regulators and backstop protections.

But, the onset of cryptocurrencies means once a thief has the asset, it's theirs.

Alex Stamos, Stanford University professor and former Facebook security chief, told an audience at our recent Franklin Templeton investor conference: "If you're investing in cryptocurrency, you absolutely have to ask them about their security because the moment they lose control of their private key for 17 milliseconds, that's it. They're out of business. There are none of the systems that we have in the global banking system, that allow banks to fail gracefully. Bitcoin and other cryptocurrencies fail immediately in a way that can't be undone."

> **"There are two types of company: companies that know they have been hacked and companies that do not know they've been hacked."**
>
> **Misha Glennyn**
> Journalist and Author

Fighting back: The role of cybersecurity

In an interconnected world, cyber has become the fifth frontier of war (after land, sea, air and space).

As an example, around three-quarters of Americans see cyberattacks from other countries as a top threat to the United States, according to a 2019 survey from the Pew Research Center.[5] When asked to choose what they saw as a top threat to the United States among a list of potentials, more Americans chose cyberattacks than Islamic State, climate change, North Korea's nuclear program, Russia, China or the condition of the global economy.

For better or worse, "smart cities" are coming—the more connected to the physical world they are, the more vulnerable they are to cyberattacks. If a government can lose control of the systems controlling its dams, nuclear reactors and power systems, it can lose its country. That becomes an existential issue.

Where lies the responsibility?

So, who's responsible for cyber defense?

For many countries around the world, the responsibility lies with a branch of law enforcement services. In the United States, for example, until recently, it was the responsibility of the Federal Bureau of Investigation (FBI). Typically, law enforcement officers are trained to watch events unfold, take very detailed notes and then to indict the people responsible afterward.

As Alex Stamos, Stanford University professor and former Facebook security chief, explained at a Franklin Templeton-hosted seminar earlier this year, that model does not work for preventing cyberattacks. He urged governments around the world to be a lot more thoughtful about engaging with necessary trade-offs.

"We can no longer have people saying that we want everything all the time. Instead, we need to highlight the specific trade-offs we want to make and identify what we're willing to give up to get them."

"That's something that has to start with citizens. Citizens have to think about who they want to be responsible. If they say they want tech companies to fix something, then they will have to give them the power that is inherent in that."

> **"Anytime the pace of change externally is greater than the pace of change internally, you're falling behind."**
>
> **Daniel Schulman**
> Chief Executive
> PayPal

Who guards the guards?

But Alex Stamos warned that while it may be easy to hand over responsibility, taking away those controls later can be more difficult.

"I think one of the things we're not really engaging in with too much is, as we create a little bit of a nanny state, these nannies are not going away. And we're setting a precedent for these half-trillion or trillion-dollar corporations to be embedded in our lives."

"We want the outcomes, but we're not thinking through what we need to do to get there. I think this is going to be one of the biggest political discussions once people start to realize the kinds of trade-offs that they're dealing with."

The threats have been significant enough for the US government to launch the Department of Homeland Security's new Cybersecurity and Infrastructure Security Agency. Nation states, with ample resources, are aggressively launching attacks to steal secrets and for financial gain. In tandem, the increasing availability of attack tools—including their very own dark-web "hacker networks" and cloud services—allow even novices to wreak havoc.

The corporate response to cybersecurity

At our recent conference, PayPal's Chief Executive Daniel Schulman told delegates his mantra: "Anytime the pace of change externally is greater than the pace of change internally, you're falling behind."

And Schulman also had words of warning: "Change is incredibly difficult for any corporation to do constantly. You can't stop for a second. I think if we really want to be great leaders, or invest in the right leaders, we really need to define this reality very brutally and then figure out how do we use these trends to do good things in the world."

Regulation will likely have a role to play. Schulman told Franklin Templeton's audience that companies could potentially garner a competitive advantage by thinking about how they value consumers' right to privacy.

"I like challenging business models and understanding what really adds competitive advantage going forward. And I think sometimes we shouldn't underestimate how important privacy is, and how important financial health is to our democracy," Schulman said.

Fundamental trade-offs

Companies, now forced to continuously scan their technology and network traffic for anomalies, also spend huge amounts of time and money teaching employees how to guard against cyberattacks. Training is critical as these attacks can disrupt business operations, abscond with intellectual property, damage in-house technology and harm corporate reputations.

The typical enterprise has well over a dozen discrete cybersecurity solutions that create another glaring problem—the complexity makes it difficult to understand what's working and what's not. Turns out, building a common-sense defense isn't easy, as hackers always seem to stay one step ahead of our collective effort to stop them.

Most corporate security teams are focused on putting out random fires and have little time for the strategic thinking and process improvement new threats require. As a result, cumbersome manual processes and blind spots expose many corporations' networks.

Cyber escalation: Adapting to the growing threat

Cybercrimes are picking up speed. The response needs to as well. Hackers who seek to install malware use automated techniques to constantly prowl smartphones, home sensors, servers, Wi-Fi routers and other equipment for vulnerabilities.

With the advent of fifth-generation technology, the problem will likely intensify. And with consumers' skyrocketing demand for IoT devices, manufacturers are often rushing new gear to market with inadequate security. While protections lag, cybercriminals race ahead.

Though it may seem counterintuitive given the benefits, automation itself is a threat. Rapid technological advances enable machines to perform a growing number of tasks traditionally done by humans using artificial intelligence (AI)—sophisticated computer programs that can learn from experience.

According to the National Bureau of Economic Research, from 1990 to 2007, robots replaced about 670,000 jobs in the United States alone, mostly in manufacturing; every robot introduced into a local economy claimed 6.2 jobs.[6] But this isn't a trend that's confined to the United States, in our view.

That trend will accelerate over the next decade as advances in mobile technology, AI, data transfer and computing speeds allow robots and drones to act with greater independence. As these intelligent machines move beyond the factory floor and integrate more deeply with society, the need for robotic cybersecurity will become paramount as people seek to forestall the kind of worst-case-scenario that was once reserved for the surreal plotline of an Isaac Asimov sci-fi novel.

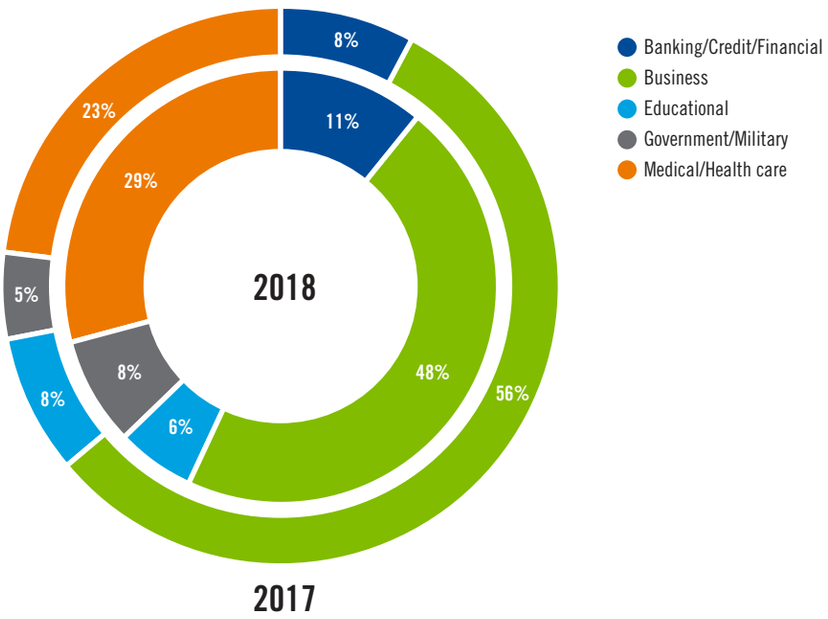
Quantum-computing researchers say they are developing revolutionary, ultra-powerful (and still experimental) machines that will have the ability to break current encryption within a decade. Security experts are in a critical race to come up with new ways to protect data before it's too late. Foreign powers could crack a significant portion of the sensitive data we have in the not-too-distant future, and there may not be much we can do to change this outcome.

Public-to-private developments

We have noticed mounting investor interest in the IT sector (indicated by rising market capitalizations among these companies), and we expect this trend to continue. Yet, one oft-cited benefit of productivity growth tied to workers' ability to utilize emerging technologies and machines efficiently remains unimpressive. Investment opportunities may exist in companies and sectors (outside of IT) that can effectively deal with cyberattacks or use technology to help improve productivity growth.

It's quite common for technological advances that originated as military applications to find their way into our everyday lives. For example, the military developed the finger-recognition technology that allows a smartphone owner to use his or her fingerprint as a password. (The technology went

UNITED STATES DATA BREACHES BY INDUSTRY



Source: Identity Theft Resource Centre.

mainstream after a large smartphone company bought the firm that invented this technology.) We believe the facial-recognition technology currently employed by the military will likely end up allowing consumers to unlock their tablet computers with a faceprint in the near future.

Patching up the holes: Cybersecurity crisis is a key anxiety of the modern age

The job of security consultants is to test a company's cyber defenses.

Along the way, they often find that the weakest link into our computers isn't the software. It's us. Hackers understand social engineering—the idea that you can break into a system by manipulating people rather than code. Ask any cybersecurity expert—it's tough to get people to behave in a particular way.

To avoid becoming an unpleasant statistic, companies have begun training for employee awareness and protocol while cataloging, tracking and "penetration testing" all their technology. By using sophisticated security information and event management tools, they have begun to automate their enterprise cybersecurity defenses just as cybercriminals have automated their attacks.

As we head into the US presidential election in 2020, we expect much more scrutiny on the measures taken by US government agencies to improve their cybersecurity measures.

We believe established leaders in the cybersecurity space, including defense companies, could be poised to benefit from such an initiative—as could the private sector. The "military-grade" cybersecurity technology we expect will likely be developed in this endeavor may eventually become the standard for the private sector. We think this technology will likely be a boon to the financials and utilities sectors, which tend to be more vulnerable to cyberattacks than others.

Technological advances have been made across a variety of industries—and we think they are not likely to stop any time soon.

Endnotes

1. Source: Center for Strategic and International Studies (CSIS). Economic Impact of Cybercrime—No Slowing Down. February, 2018.
2. Source: ThreatMetrix Cybercrime Report 2017: A Year in Review, January 2018.
3. Source: Symantec 2019 Internet Security Threat Report.
4. Source: FireEye "M Trends Report" for 2019.
5. Source: Pew Research Center: Global Attitudes and Trends, February 2019.
6. Source: National Bureau of Economic Research. Robots and Jobs: Evidence from US Labor Markets. March 2017

Contributors

Jonathan Curtis
Research Analyst,
Franklin Equity Group®

James Cross, CFA
Research Analyst,
Franklin Equity Group®

WHAT ARE THE RISKS?

All investments involve risks, including possible loss of principal. Investing in fast-growing industries, including the technology sector (which has historically been volatile) could result in increased price fluctuation, especially over the short term, due to short product cycles, falling prices and profits, competition from new market entrants and development and changes in government regulation of companies emphasizing scientific or technological advancement as well as general economic conditions. Growth stock prices reflect projections of future earnings or revenues, and can, therefore, fall dramatically if the company fails to meet those projections. Buying and using a blockchain-enabled cryptocurrency, such as bitcoin, carries risks. Speculative trading in cryptocurrencies, many of which have exhibited extreme price volatility, carries significant risks. Among other risks, interactions with companies claiming to offer cryptocurrency payment platforms and other related products and services may expose users to fraud. Blockchain technology is a new and relatively untested technology and may never be implemented to a scale that provides identifiable benefits. Investing in cryptocurrencies and ICOs is highly speculative, and an investor can lose the entire amount of their investment. If a cryptocurrency is deemed a security, it may be deemed to violate federal securities laws. There may be a limited or no secondary market for cryptocurrencies.

IMPORTANT LEGAL INFORMATION

This material is intended to be of general interest only and should not be construed as individual investment advice or a recommendation or solicitation to buy, sell or hold any security or to adopt any investment strategy. It does not constitute legal or tax advice.

The companies and case studies shown herein are used solely for illustrative purposes; any investment may or may not be currently held by any portfolio advised by Franklin Templeton Investments. The opinions are intended solely to provide insight into how securities are analyzed. The information provided is not a recommendation or individual investment advice for any particular security, strategy, or investment product and is not an indication of the trading intent of any Franklin Templeton managed portfolio. This is not a complete analysis of every material fact regarding any industry, security or investment and should not be viewed as an investment recommendation. This is intended to provide insight into the portfolio selection and research process. Factual statements are taken from sources considered reliable, but have not been independently verified for completeness or accuracy. These opinions may not be relied upon as investment advice or as an offer for any particular security. **Past performance does not guarantee future results.**

The views expressed are those of the investment manager and the comments, opinions and analyses are rendered as at publication date and may change without notice. The information provided in this material is not intended as a complete analysis of every material fact regarding any country, region or market.

Data from third party sources may have been used in the preparation of this material and Franklin Templeton Investments ("FTI") has not independently verified, validated or audited such data. FTI accepts no liability whatsoever for any loss arising from use of this information and reliance upon the comments opinions and analyses in the material is at the sole discretion of the user.

Products, services and information may not be available in all jurisdictions and are offered outside the U.S. by other FTI affiliates and/or their distributors as local laws and regulation permits. Please consult your own professional adviser or Franklin Templeton institutional contact for further information on availability of products and services in your jurisdiction.

Issued in the U.S. by Franklin Templeton Distributors, Inc., One Franklin Parkway, San Mateo, California 94403-1906, (800) DIAL BEN/342-5236, franklintempleton.com—Franklin Templeton Distributors, Inc. is the principal distributor of Franklin Templeton Investments' U.S. registered products, which are not FDIC insured; may lose value; and are not bank guaranteed and are available only in jurisdictions where an offer or solicitation of such products is permitted under applicable laws and regulation.

Australia: Issued by Franklin Templeton Investments Australia Limited (ABN 87 006 972 247) (Australian Financial Services License Holder No. 225328), Level 19, 101 Collins Street, Melbourne, Victoria, 3000. **Austria/Germany:** Issued by Franklin Templeton Investment Services GmbH, Mainzer Landstraße 16, D-60325 Frankfurt am Main, Germany. Authorised in Germany by IHK Frankfurt M., Reg. no. D-F-125-TMX1-08. Tel. 08 00/0 73 80 01 (Germany), 08 00/29 59 11 (Austria), Fax: +49(0)69/2 72 23-120, info@franklintempleton.de, info@franklintempleton.at. **Canada:** Issued by Franklin Templeton Investments Corp., 5000 Yonge Street, Suite 900 Toronto, ON, M2N 0A7, Fax: (416) 364-1163, (800) 387-0830, www.franklintempleton.ca. **Netherlands:** FTIS Branch Amsterdam, World Trade Center Amsterdam, H-Toren, 5e verdieping, Zuidplein 36, 1077 XV Amsterdam, Netherlands. Tel +31 (0) 20 575 2890. **United Arab Emirates:** Issued by Franklin Templeton Investments (ME) Limited, authorized and regulated by the Dubai Financial Services Authority. Dubai office: Franklin Templeton Investments, The Gate, East Wing, Level 2, Dubai International Financial Centre, P.O. Box 506613, Dubai, U.A.E., Tel.: +9714-4284100 Fax: +9714-4284140. **France:** Issued by Franklin Templeton France S.A., 20 rue de la Paix, 75002 Paris France. **Hong Kong:** Issued by Franklin Templeton Investments (Asia) Limited, 17/F, Chater House, 8 Connaught Road Central, Hong Kong. **Italy:** Issued by Franklin Templeton International Services S.à.r.l. – Italian Branch, Corso Italia, 1 – Milan, 20122, Italy. **Japan:** Issued by Franklin Templeton Investments Japan Limited. **Korea:** Issued by Franklin Templeton Investment Trust Management Co., Ltd., 3rd fl., CCMM Building, 12 Youido-Dong, Youngdungpo-Gu, Seoul, Korea 150-68. **Luxembourg/Benelux:** Issued by Franklin Templeton International Services S.à r.l. – Supervised by the Commission de Surveillance du Secteur Financier - 8A, rue Albert Borschette, L-1246 Luxembourg - Tel: +352-46 66 67-1 - Fax: +352-46 66 76. **Malaysia:** Issued by Franklin Templeton Asset Management (Malaysia) Sdn. Bhd. & Franklin Templeton GSC Asset Management Sdn. Bhd. **Poland:** Issued by Templeton Asset Management (Poland) TFI S.A.; Rondo ONZ 1; 00-124 Warsaw. **Romania:** Issued by Bucharest branch of Franklin Templeton Investment Management Limited ("FTIML") registered with the Romania Financial Supervisory Authority under no. PJM01SFIM/400005/14.09.2009, and authorized and regulated in the UK by the Financial Conduct Authority. **Singapore:** Issued by Templeton Asset Management Ltd. Registration No. (UEN) 199205211E. 7 Temasek Boulevard, #38-03 Suntec Tower One, 038987, Singapore. **Spain:** FTIS Branch Madrid, Professional of the Financial Sector under the Supervision of CNMV, José Ortega y Gasset 29, Madrid, Spain. Tel +34 91 426 3600, Fax +34 91 577 1857. **South Africa:** Issued by Franklin Templeton Investments SA (PTY) Ltd which is an authorised Financial Services Provider. Tel: +27 (21) 831 7400, Fax: +27 (21) 831 7422. **Switzerland:** Issued by Franklin Templeton Switzerland Ltd, Stockerstrasse 38, CH-8002 Zurich. **UK:** Issued by Franklin Templeton Investment Management Limited (FTIML), registered office: Cannon Place, 78 Cannon Street, London EC4N 6HL Tel +44 (0)20 7073 8500. Authorized and regulated in the United Kingdom by the Financial Conduct Authority. **Nordic regions:** Issued by FTIS Stockholm Branch, Blasieholmsgatan 5, SE-111 48, Stockholm, Sweden. Tel +46 (0)8 545 012 30, nordicinfo@franklintempleton.com FTIS is authorised and regulated in the Luxemburg by the Commission de Surveillance du Secteur Financier and is authorized to conduct certain financial services in Denmark, in Sweden, in Norway and in Finland. **Offshore Americas:** In the U.S., this publication is made available only to financial intermediaries by Templeton/Franklin Investment Services, 100 Fountain Parkway, St. Petersburg, Florida 33716. Tel: (800) 239-3894 (USA Toll-Free), (877) 389-0076 (Canada Toll-Free), and Fax: (727) 299-8736. Investments are not FDIC insured; may lose value; and are not bank guaranteed. Distribution outside the U.S. may be made by Templeton Global Advisors Limited or other sub-distributors, intermediaries, dealers or professional investors that have been engaged by Templeton Global Advisors Limited to distribute shares of Franklin Templeton funds in certain jurisdictions. This is not an offer to sell or a solicitation of an offer to purchase securities in any jurisdiction where it would be illegal to do so.

Please visit www.franklinresources.com to be directed to your local Franklin Templeton website.

CFA® and Chartered Financial Analyst® are trademarks owned by CFA Institute.

FRANKLIN TEMPLETON