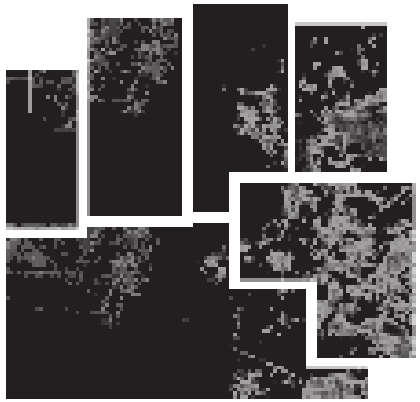
A Manifesto for Cyber Resilience



Unknown
Unknowns
Cyber Defined
BYOD
Fighting
Yesterday's
battles
Revolutionaries
Understand
where you stand
Human Factor
Employee Threat
Cyber Resilience

Cyber Resilience Defined

Some 2.4 billion global Internet users—34 percent of the world's population—spend increasing amounts of time online.[1] As our online activity expands, it isn't just creating new ways to do business. It's revolutionizing business. However, like any mass movement with significant ramifications, the Internet-enabled life has risks as well as benefits. Some are willing to accept those risks without much consideration. Others want to take the time for a more contemplative response, but events are moving too quickly for long debate. What we really need is a Call to Action that addresses the risks demanding urgent attention.

To balance the benefits of the digital life, management needs to understand and grapple with four equally powerful forces:

Democratization – The way customers insist on interacting via the channels they prefer, rather than the channels the organization imposes.

Consumerization – The impact of the many devices and applications that span work and play in our digital lives.

Externalization – The ways in which cloud computing slashes capital expenditure and shakes up how data moves in and out of organizations.

Digitization – The exponential connectivity created when sensors and devices form the "Internet of Things." These forces interact in ways that make eradicating Cyber Risk impossible; eliminating it in one area simply shifts it to the others.

However, by following best practices, it is possible to reduce your organization's exposure to Cyber Risk across the board. By addressing the real and growing risks we face as individuals, businesses, and governments, we can begin to create an optimal environment of Cyber Resilience. This Manifesto sets out a road map for that process.

What We Know Today

Digital technology has become so inextricably woven into our daily lives that doing without it has become as unthinkable as going back in time. What bank customer would be willing to give up the ability to transfer money—even across international borders—in milliseconds? What businessperson would return to buying airline tickets at a counter or placing business calls from a phone booth? And with the advent of 3-D printing, what manufacturer would pay shipping for a component it could print onsite?

The rise of mobility is only accelerating these trends. Although only 15 percent of the world's Internet traffic is currently mobile, that figure is growing fast: of the world's 5 billion mobile phones, a third are Internet-enabled smartphones whose users share 500 million photos daily and check their messages an average of 23 times a day.[1]

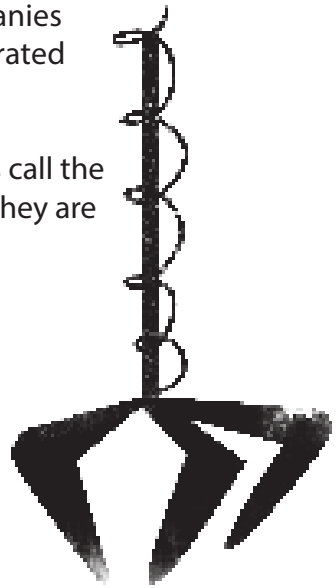
Yet the complex, fast-moving transactions technology enables are also a potential minefield for businesses.

Online attacks claim 1.5 million victims every day and add up, conservatively, to $110 billion in losses each year.[2] Malware, or malicious software attacks, on the web increased 23 percent in 2013 and on mobile devices grew 139 percent in the same period.[3] Crucially, of the websites serving up malware, 67 percent were from legitimate sites that had been compromised.[3]

Worried yet?

As desktop computer operating systems give way to web-based and mobile platforms and applications, criminals are evolving new digital threats to keep pace. They're also expanding their targets to include organizations that lack the levels of security found in the largest enterprises. Far from flying under the radar of online threats, smaller companies are more exposed than ever: 41 percent of attacks affect organizations with fewer than 500 employees.[2] And while larger organizations may think themselves well-protected, this focus on smaller companies may result in their supply chain being infiltrated from below.

As a result, changes in what security experts call the "threat landscape" are as hard to predict as they are to address.



The Unknown Unknowns

It is literally impossible to predict all the online threats your organization will face, so your best hope of combating them is to prepare for any possibility. The people creating the threats may be criminals, terrorists, state-sponsored cyberspies, or disgruntled "hacktivists." Their motivations could be anything from peaceful protest to malicious intent, political advantage to financial gain, or any combination thereof.

What's more, their ability to create and unleash digital chaos is increasing exponentially. Only the most knowledgeable of security experts have the level of expertise shared in the "black economy." Your law-abiding organization is unlikely to receive a backstage pass to this underground world where hackers exchange stolen data, sell ready-made malware kits, and develop new ways to secure their operations.

The Human Factor

While 84 percent of data breaches occur in hours or less, two-thirds aren't discovered for months, and 22 percent of us don't manage to contain them for months or even years.[4] Why is this?

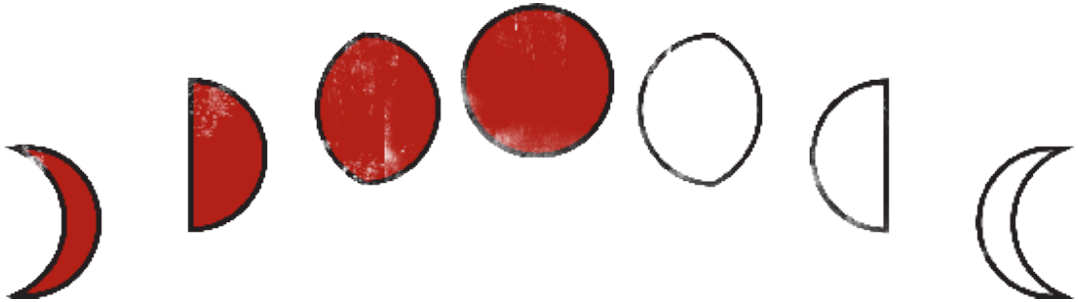
It isn't a lack of technology. The newest, fastest, shiniest hardware or software can be necessary for your company's digital security, yet still not sufficient to ensure it. It's the human factor—the person reading this manifesto—that introduces the greatest risk. You and I are the weakest link.

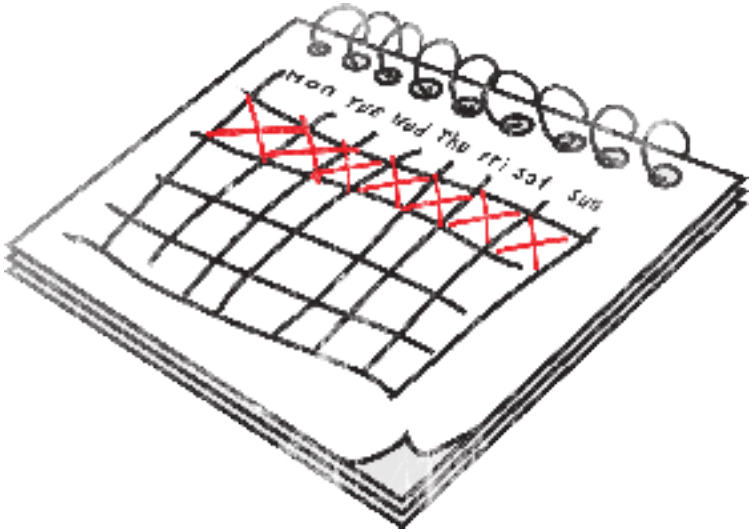
Part of the problem is IT's changing role within the organization. Although IT touches every department and traditionally has primary responsibility for data security, its ability to control what technology the organization uses is slipping. While IT may still be a trusted advisor in purchasing technology, it's no longer the gatekeeper: Recent research shows that 14 percent of cloud storage, 13 percent of social media, and 11 percent of office productivity software is implemented without the IT department's knowledge.[5] In addition, Gartner data shows the movement of IT spending to other departments is already well under way. The marketing department is a front-runner and due to outspend the IT department on technology by 2017.[6]

In short, the human element of Cyber Risk within your organization is likely to be higher outside your IT department within it. As a result, concentrating data security knowledge and expertise in IT actually increases your risk, while spreading the expertise—making your security culture all-inclusive—is a worthwhile strategy for reducing it.

84% initial compromises take hours or less

66% breaches are not discovered for months





22% breaches take months or longer to contain

Risk 1 Businesses Are Small Compared to the Threat

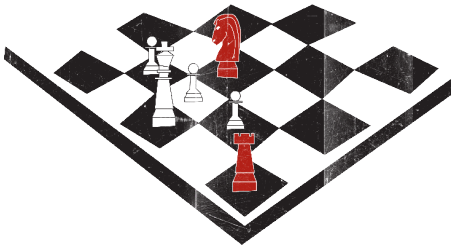
Few organizations—even global multinationals—have the resources to stay on top of all the digital threats a highly motivated team of attackers can mount. The bad guys are also smart guys. They already have years of experience collaborating in virtual teams across national boundaries for mutual benefit, selling tricks to each other and trading stolen identities. They're launching today's cross-boundary, cross-platform attacks against security systems built for yesterday's pre-cloud, pre-mobile, and sometimes even pre-Web, nation-based world.

Most cyberattacks remain comparatively unsophisticated, and all but 10 percent of organizations have enough security basics in place to fend them off. However, 78 percent of organizations use only the basic security resources available online, with no customization.[4] This leaves them vulnerable to more sophisticated attacks—especially under the traditional approach of buying more security tools piecemeal. Organizations need to obtain greater visibility into their organization's current security stance and react accordingly.

Moreover, as organizations pursue efficiency by linking ever more systems together, using smart meters to manage energy use, sensors to control production lines, and RFID tags to track shipments, attackers have an increasing number of targets at their disposal—targets that aren't in the IT department, nor even human. Only a handful of organizations, primarily in the defense sector, have the bandwidth to spend all their time fighting digital threats. The rest of us, processing insurance claims or selling shoes or servicing cars, have to spend wisely to become more Cyber Resilient—and, more importantly, we have to follow our attackers' lead. By banding together as the global community of "black hats" have already done, we can pool resources, share knowledge about the severity of threats, and maybe even make it a fair fight.

Risk 2 Fighting yesterday's battles loses the war

As risks to data security have become more subtle, personalized, and distributed, detecting them has become increasingly difficult—it is impossible to claim any IT system connected to the Internet (which is to say, virtually all of them) is impregnable. It isn't just that human intelligence almost always bypasses a "wall of steel." Today's smarter, more sophisticated threats aren't blunt full-frontal assaults. They're personalized. They attack many vulnerabilities at once. And when they succeed, they're more devastating. Today's attackers can plant a payload by web, email, or mobile, then awaken it from hibernation to create a zombie botnet that remains on the infected system even after the infection is detected and the method of infection eliminated. Yesterday's approach to data security, the isolated removal of threats, needs to evolve into a slow, determined, ongoing process of Cyber Resilience. Instead of trying to block attacks, Cyber Resilience is about making you a less attractive target: making access to your systems difficult enough and unprofitable enough to steer attackers to lower-hanging fruit. With a deeper understanding of the threats your organization faces, your organization can assess its risks, choose the ones it's willing to take in pursuit of strategic advantage, and build its defenses accordingly.



Risk 3 Ignoring the role of Employees

Employees are often cited as the greatest asset an organization has. The reality is they can also be the greatest liability from a security point of view. Identity theft and the physical theft of unprotected devices, often encouraged by today's generous BYOD policies, greatly complicate matters.

Where once security was the sole responsibility of IT professionals, the pervasiveness of "shadow IT" means it cannot be left to them alone. One person's non-sanctioned technology spending is another's fast track to innovation, and if IT professionals crack down on them aggressively, they're likely to be seen less as protectors of data than as hindrances to productivity.

Critically, research indicates that 53 percent of employees believe that taking corporate data "doesn't harm the company,[7] and 35 percent of all data breaches originate internally, particularly with individuals preparing to leave the organization.[8] To address this, organizations need to train non-technical employees in their security processes as well as the ramifications and consequences of ignoring them. By helping employees make wiser decisions about the use of technology, organizations can reduce unintentional malpractice and increase the organization's Cyber Resilience. This is not an abdication of IT's responsibility; it is, rather, a chance to convert IT expertise into competitive advantage. The idea is to empower non-technical employees and reduce non-intentional malpractice.

Far from being an abdication of responsibility by IT, here is a chance to convert IT expertise into competitive advantage. There is a new deal to be struck between non-IT professionals and their more technical IT colleagues, showing them how Cyber Resilience can increase their organization's potential. In Cyber, ignorance is not bliss – it's a communication and an organizational challenge. In other words an untapped commercial opportunity.

How To Become Cyber Resilient 1

Understand where your organization stands

A well-known management saying is "You cannot manage what you cannot measure." However, most cyber attacks go unnoticed, never mind measured, as are the risks they pose.[4] How can we then assess our level of risk?

The journey to Cyber Resilience should start with a comprehensive external assessment of the people, processes, and products involved in data security:

- Establish a baseline with an independent audit of the technology and processes your organization uses as well as the vulnerabilities in your security stance
- Develop a benchmark to compare your results to that of your peers
- Conduct a gap analysis between where you are and where you want to be to develop practical, strategic recommendations

By taking these steps, you begin to transform your "unknown unknowns" into visible action items and prioritize them, not just for your IT department, but also across the entire organization. Your analysis reveals the organization's vulnerabilities, helps you spot the most urgent and/or pressing issues first, and suggests ways to address them and thus make your organization less appealing as a target for attackers.

How To Become Cyber Resilient 2

Coaching your colleagues, ALL of them

Once upon a time, computers were hard to move, difficult to use, and managed by only a few people. Things have changed. Now your employees can carry business-critical, confidential data in their pockets—and so can employees of your business partners, and their business partners, and so on. The genie of data is out of the bottle, and your best practices for on-premise data security can only protect you to the extent that the least secure person in possession of your data follows them. Writing and enforcing password policies, locking down devices, and complying with ISO standards will only boost your Cyber Resilience if you can ensure everyone from your contract cleaners and external caterers to your auditors and attorneys also adheres to the same policies.

As already mentioned, analysts predict that in the near future, more IT spending will take place outside of IT than within it—and even people who have spent their entire careers in IT are unlikely to be prepared for the continuing changes the explosive growth of Internet-enabled technology is bringing to the business world. It's time to think outside of the box, outside of the IT department, outside of job descriptions, and outside of your organizational boundaries.

Drop the tech speak, drop the security jargon, and reach out to your colleagues—all of them. Everyone who works with your organization needs to understand what digital security is, why it's important, and what they need to do to uphold it.

How To Become Cyber Resilient 3

Make Cyber Resilience your competitive advantage

Your enemies are many, unseen, and clever, made of components that can form, morph, and dissolve fluidly as needed. Don't try to battle them alone. Join forces with other organizations that share your security concerns. Pool your IT security intelligence and skills to develop joint strategies that can flex and scale with the constant, ever-changing nature of the threat. A security vendor with a comprehensive security intelligence network provides a holistic overview of emerging threats across companies, industries, and continents, while an incident response service offers expertise when you need it.

Instead of putting out fires and being the one to blame when things go wrong, IT at the heart of a Cyber Resilient organization is proactive, gathering security intelligence from existing security controls and technologies that already exist in your environment. This intelligence allows you to not only respond to attacks, but also to gauge the organization's ability to fend off threats so executive leaders can make well-informed decisions regarding their cyber security strategy.

Conclusion

Futurist and novelist Arthur C. Clarke famously wrote, "Any sufficiently advanced technology is indistinguishable from magic." The online revolution has produced results that just a few years ago would have been virtually magical, all because of the ability to send and receive data securely. That security has become too central to our daily lives not to take with the utmost seriousness—the same level of seriousness we give to power, water, talent, and other vital real-world inputs on which the comforts of our personal lives and the stability of our global systems depend.

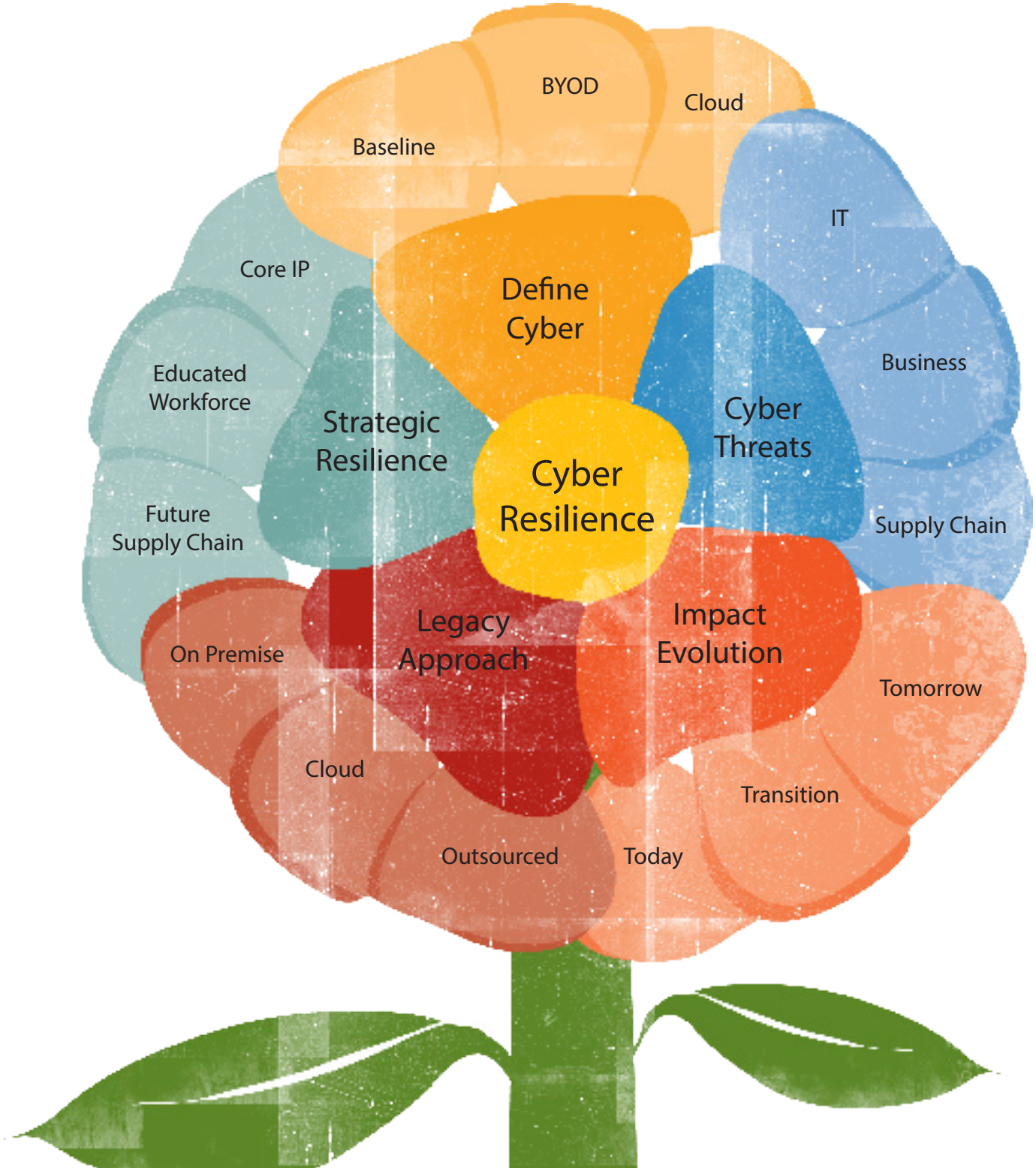
No top-down edict is enough to mitigate the risks; technology moves too fast. Only an informed but flexible grass roots movement can keep up with the threats to our digital assets. It's up to you and other IT professionals to lead the way:

1. Setting a baseline for your organization's current Cyber Resilience, effectively and soon.

2. Enlisting everyone in your organization's supply chain in the effort, educating him or her about the need to balance innovation with security.

3. Leveraging the concepts behind Cyber Resilience and making use of all of your security intelligence for long-term competitive advantage and protection.

We hope this Manifesto will start the chain reaction necessary to get your organization moving down the path to Cyber Resilience. If it has, contact the experts at Symantec for further assistance; our assessment and security products and services can help you take the next steps.


BYOD
Cloud
Baseline
IT
Core IP
Define Cyber
Business
Educated Workforce
Strategic Resilience
Cyber Threats
Cyber Resilience
Future Supply Chain
Supply Chain
Legacy Approach
Impact Evolution
On Premise
Tomorrow
Cloud
Transition
Outsourced
Today

References

Unstoppable movements start revolutions. Our products and services are acknowledged to be at the leading edge of Cyber knowledge and Symantec would like to engage with your Cyber efforts.

Share today, be part of the resistance.

1 – Mary Meeker, KPCB, 2013 Internet Trends

2 – Norton Cybercrime Report

3 – Symantec ISTR 2013

4 – Verizon DBIR 2013

5 – Economist Intelligence unit July 2013 'Security Empowers Business – unlock the power of a protected enterprise'

6 – Gartner Webinar January 2013 'By 2017 the CMO will spend more than the CIO' by Laura McLellan

7 – Symantec 'What's Yours is Mine: How Employees are Putting Your IP at Risk' paper 2013

8 – Symantec 'Cost of a Data Breach Study 2013'

Contacts

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA

www.symantec.com

Symantec protects the world's information, and is a global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/cyber-resilience.