SPRING 2020 / ISSUE NO.16

$ 15.00 | € 10.00 | 1500 RSD

# HORIZONS

JOURNAL OF INTERNATIONAL RELATIONS AND SUSTAINABLE DEVELOPMENT

## PANDEMICS & GEOPOLITICS
## THE QUICKENING

UNLOCKING THE MIDDLE EAST

SUSTAINABLE CYBERSPACE

ISSN 2406-0402

ABDELAL • BREMMER • BROS • DAVUTOĞLU • DUCLOS • DURBIN
FAHMY • FEDOROV • FRIEDMAN • HEISTEIN • HOFMAN • KORTUNOV • KUMAR
MUKERJI • RUBIN • SACHS • SARIOLGHALAM • SINGH • TERZIC • YADLIN

cirsd.org

# Security Means Business

Steve Durbin

OFTEN attributed, incorrectly, to being a Chinese saying, "may you live in interesting times" is a phrase one hears invoked frequently nowadays. Whether Chinese, American, or simply invented, I don't think that anyone would argue that we are indeed living today in "interesting times." Over the past few months, almost every email in my inbox is an update from people and companies with whom I do business, advising me of their most recent response to COVID-19. My news streams also are filled with headlines of the latest developments. It's hard to think of comparable major crisis to which we as business people have had to respond both globally and ongoing. "Interesting times" indeed.

As someone responsible for an organization whose sole reason for existing is to support its members to predict, assess, and mitigate against threats and manage risk, one of my anxieties amid this unfolding "interesting times" scenario is to the business vulnerability inherent in the situation. Most of us have had to scramble to achieve business continuity at the same time as we guard our own and our staff's health. Many of us have had to shift our enterprises to be largely home-working.

To put it simply, COVID-19 has driven up our level of risk significantly; the introduction of more threats has immensely increased the opportunity for cybercriminals to take advantage of our moments of distraction.

Without scaremongering, I want to use this essay as an opportunity to lay out some of the risks that I now see. There were and continue to be enough challenges, given the complexities of the technological, regulatory, and geopolitical playing fields upon which we operate. COVID-19 has just shone a light on them. I aim to underscore that business leaders need to make sure that security is firmly on their respective radars. More than that, that they understand "security" as less of a separate function within their businesses, and more of a top-to-bottom, end-to-end, people-enabled activity that will make a significant difference to the long-term success of their companies.

> *COVID-19 has driven up our level of risk significantly; the introduction of more threats has immensely increased the opportunity for cybercriminals to take advantage of our moments of distraction.*

## Cyber Culture

"What's the big deal?" one might ask. Why is it that in the United States over half of CEOs are extremely concerned about the impact of cyberthreats on their ability to grow their businesses, according to PwC's Global CEO Survey?

To understand the inherent threat, first we need to look at how cyber itself is evolving. And, indeed, how our blurring of work and life, together with our social media-based "share all" culture, is opening for attack doors that were once firmly closed.

Although no one is feeling nostalgic about it, there was a time, not terribly long ago, when conducting cyber mischief was a personal enterprise—typically, a lonely teen operating out of his or her home basement or bedroom. But today, in the eyes of institutions eager to secure sensitive digital files, the solitary teenage hacker is less a problem than a nuisance.

What has mostly taken his place—and the overwhelming majority of hackers are male—are well organized, highly-resourced criminal enterprises, many of which operate outside the boundaries of a given business's jurisdiction, with the ability to monetize stolen data on a scale rarely, if ever, achieved by the bedroom-based hacker. The most persistent of them—and the hardest to defend against—are state-sponsored. But it is among young people that cyber-culture, including its more malevolent forms, is spread and nourished. And they don't need to be thugs to participate.

As a McKinsey report in October 2019 highlighted, cyber threats are increasing in capacity and frequency, with a low cost of entry and a variety of capability (Figure 1).

Furthermore, according to a recent Juniper Research report, the total cost to businesses of data breaches is

*Steve Durbin is the Managing Director of the Information Security Forum (ISF), a Fellow of the Chartered Institute of Marketing, and a Visiting Lecturer at Henley Business School, having formerly served at Ernst & Young and been Senior Vice President at Gartner. You may follow him on Twitter @stevedurbin.*

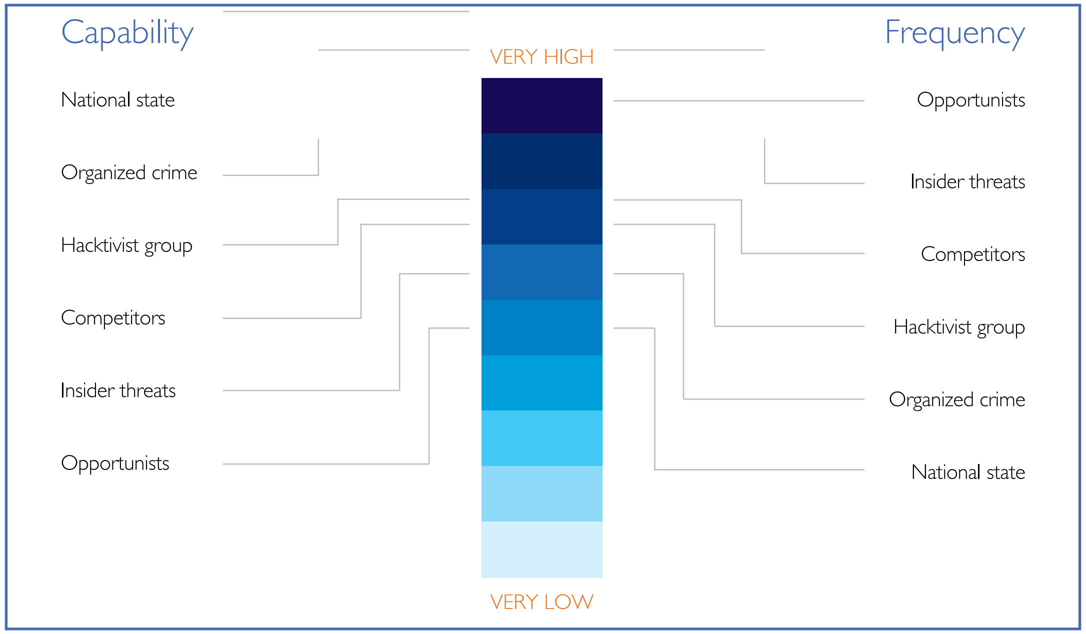

*Figure 1: Cyberthreat Capacity and Frequency Today—Threat Actor*

Source: McKinsey & Company, The risk-based approach to cybersecurity, October 2019

expected to increase nearly 70 percent over the next five years, from $3 trillion in 2019 to more than $5 trillion in 2024. And, of course, breaches don't just wreak significant financial damage. They cause considerable damage to brand reputation too. And that's often very difficult to win back.

But unlike bank robberies of years past, cyber-theft bypasses the need to confront victims with threats of harm to coerce them to hand over money. In fact, at the end of 2013, the British Bankers Association reported that "traditional" strong-arm bank robberies had dropped by 90 percent since 2003. And the yield has also dropped significantly, the average return on bank robbery in 2016 being $4,500. Contrast that with attacks on four cryptocurrency exchanges, which in 2018 yielded $773 million. Cyber crime certainly pays.

Furthermore, with just a few keystrokes, the larcenous acts themselves, which produce neither injury nor fear, seem almost harmless. And, at least in the eyes of adolescent perpetrators—eyes which are frequently hidden behind a mantle of anonymity and under the influence of lawless virtual worlds that populate immersive online games—the slope leading from cyber mischief into cyber crime is very gradual and hard to discern.

In fact, malice is not even what typically motivates young people to become hackers; having fun is. A recent story in *The Guardian* profiling a Belarusian cyber criminal, operating online under the *nom de guerre* Policedog, is typical. Growing up in Minsk, he became involved in cyber mischief at 13, although like many of his peers, he didn't consider what he was doing to be criminal. It was a game, he told the reporter. What he really wanted was a paying job. But, over time, the game took on a darker aspect. By age 20, he had emerged as a master at turning stolen credit card information into cash, claiming to have earned $100,000 a month at his craft.

*Unlike bank robberies of years past, cyber-theft bypasses the need to confront victims with threats of harm to coerce them to hand over money.*

Other hackers have different motives: some feel challenged to probe and test the security of an institution's firewalls; others to shame, expose, or seek revenge on an acquaintance; and a few posturing as highly principled whistleblowers unmasking an organization's most sensitive secrets.

We used to think of banks and other significant institutions as safe and impenetrable. Similarly, as people, we used to keep our personal lives to ourselves. But much of that has changed, especially with the advent of smartphones. The lines between our work and home lives are now more blurred. Social media and our increasingly voyeuristic culture make us less aware of when we may inadvertently be sharing details about ourselves that the hacker in our midst is only too ready to abuse.

Examples are legion. Here, I'll stick to four.

- Earlier this year, as I was flying from Chicago to New York, I couldn't help but over hear the gentleman on the opposite side of the aisle telling his seatmate—a complete stranger—all about his recent prostate surgery.
- Attractive and aspiring celebrities regularly leak—actually, a better term for it might be that they release—videos of the most intimate moments they've had with recent lovers.
- On a packed commuter train to London before the lockdown, I sat next to someone logging into his work's computer system. Had I been so inclined, I could have used—to his and his firm's detriment—some of the personal details and company sensitive material he unwittingly revealed.
- People working for extremely sensitive government organizations self-righteously hand over the nation's most confidential data files to be posted online, purportedly to serve the public interest.

### THREE DOMINANT THREATS

If COVID-19 has taught us anything it is that there is a very real need to anticipate threats—to develop scenarios for handling them and to test our response before they cripple our businesses. With the constantly evolving threat landscape facilitated both by technological innovation and by shifts in our geopolitical landscapes right now, I see three dominant security threats for which businesses need to prepare over the coming 18 months. Let's take a look at each.

> *Critical National Infrastructure (CNI), device manufacturers, businesses, and citizens will all be heavily or totally dependent on 5G to operate. From nation-states aiming to cripple CNI to hackers spying on private networks, 5G technologies and infrastructure will become a key target.*

The first is *5G technology*. The arrival of 5G, with significantly faster speeds, increased capacity, and lower latency, will vastly enhance existing operating environments. However, these benefits will come at the expense of exponential growth of attack surfaces. The 5G-enabled devices and networks that underpin society will be compromised by new and traditional attacks, causing chaos and plunging business into disarray.

A range of industries that leverage 5G to become more operationally efficient or to automate and speed up processes will feel the impacts of attacks on 5G technologies. There will be countless opportunities to target 5G infrastructure, including billions of previously unconnected devices and new private networks.

Millions of new 5G-enabled masts, built and operated by a plethora of companies and governments to varying levels of assurance, will have new vulnerabilities exposed and create new ingress points for attackers to exploit. The step-change in available bandwidth will act as an accelerator to existing attacks and amplify new ones, stretching organizational resilience to its maximum.

Critical National Infrastructure (CNI), device manufacturers, businesses, and citizens will all be heavily or totally dependent on 5G to operate. From nation-states aiming to cripple CNI to hackers spying on private networks, 5G technologies and infrastructure will become a key target. The products produced by Chinese manufacturer Huawei are at the center of the aggressive worldwide rollout of 5G. The company's access to critical infrastructures will continue to occupy the minds of politicians and business leaders as economic tensions and protectionism continue.

The threat is real and it is headed our way. Business leaders owe it to their stakeholders to be identifying where 5G may be used across the full organizational real estate and updating and testing the efficacy of crisis management and business continuity plans in the event of 5G networks or infrastructure takedown. This will include understanding the implications of outage on our critical suppliers.

The second dominant threat is *cyber crime*, whether committed by criminals, nation-states, or the classical fifth columnist inside man. Criminal organizations have massive resource pools available to them, and there is evidence that nation-states are outsourcing as a means of establishing deniability.

Nation-states have fought for supremacy throughout history, and more recently, this has involved targeted espionage on nuclear, space, information, and now smart technology. Industrial espionage is not new and commercial organizations developing strategically essential technologies will be systematically targeted as national and commercial interests blur.

Targeted organizations should expect to see sustained and well-funded attacks involving a range of techniques. Ramsomware—so cheap and easy to access—is one of the rising areas of concern for law enforcement and businesses alike. The impact can be devastating, resulting in millions of dollars being lost not just through ransom payments but through lost customers, business disruption, and the cost of remediation.

Additionally, the insider threat is one of the most significant drivers of security risks that organizations face, as a malicious insider utilizes credentials to gain access to a given organization's critical assets. Many organizations are struggling to detect nefarious internal acts, often due to limited access controls and the ability to detect unusual activity once someone is already inside their network.

The threat from malicious insider activity is an increasing concern—especially for financial institutions—and will continue to be so in the years to come. There is no easy answer. Monitoring, the use of new technology such as artificial intelligence, and background checks are all part of the armory to respond; but the challenge remains and it is one that is already within the walls of many businesses.

The third dominant threat is the *fast and loose manner with which we treat sensitive information*. Highly sophisticated and extended supply chains, including cloud technology and our obsession with mobility (albeit currently curtailed during the current pandemic), present new risks to personal information for the simple reason that it is necessarily shared with third-parties (mobile banking, government websites, online health services, and retail, to name a few).

Since so much of our critical data is now held by third parties, this opens an opportunity for cyber criminals aiming to disrupt lives for political or monetary gain. Our information has a value, the smallest of data points can be combined to deliver a treasure trove of insight for the hacker or would-be cyber criminal.

> *How do we protect the information that we are so willingly sharing? What is the role of government and just how much personal responsibility do we all need to be taking for securing valuable information?*

So what to do? How do we protect the information that we are so willingly sharing? What is the role of government and just how much personal responsibility do we all need to be taking for securing valuable information?

Governments and legislators clearly have a role to play but there must be a balance between handing powers to the authorities to protect their citizens whilst also ensuring the protection of the individual's rights to privacy.

But what is the right balance, and how do we achieve it? It's a debate that's been going on for some time. Clearly, there is a need to protect the rights of the individual around the collection, processing, and storage of personal information. The answer, as embodied in legislation such as the European General Data Protection Regulation (GDPR) for instance, would seem to be that any such collection should only be for specified, explicit, and legitimate purposes. Also, that it be limited to what is necessary as defined by the courts and that the data once collected should not be stored for longer than is necessary.

That said, I see no near-term end to the ongoing debate over the concern with the gathering and processing of personal information, whether it be through surveillance programs such as that undertaken by America's National Security Agency or indeed more recently by other authorities around the world via facial recognition systems and drones.

The emerging practice of monitoring suspected coronavirus sufferers, whilst expedient in today's fight against COVID-19, presents a very real challenge to privacy and the rights of the individual. In the ideal world this would not be happening without first some strong, legal guidelines around the access to such information, its use, storage and destruction after use. Again, in an ideal world, privacy-by-design guidelines would be applied.

But this is not the ideal world and many governments are considering or already proceeding with such monitoring in the name of public health and safety.

> *Rolling back what many privacy campaigners will have seen as an invasion of personal privacy in the name of expediency in the wake of the COVID-19 pandemic will be the test of trust and transparency and one which some may not pass.*

There is a deeply ethical, emotional, and philosophical debate to be had—and of course, a legal one as well—around the access to and use of information that we do not have the time to undertake in these exceptional circumstances. The best the individual can hope for is transparency around the fact that monitoring is taking place, transparency around how the captured data will be used, and for what period of time.

Rolling back what many privacy campaigners will have seen as an invasion of personal privacy in the name of expediency in the wake of the COVID-19 pandemic will be the test of trust and transparency and one which some may not pass.

We live in a world of increasing surveillance, and guidelines and laws to protect the rights of the individual will need to continue to evolve to reflect the advancements that technology brings daily. Transparency and oversight are fundamental requirements and striking an acceptable balance will be an ongoing challenge in our increasingly cyber-enabled world.

## Unhelpful Business Paradigms

In addition to these threats, there are some assumptions being made about how business works that in and of themselves may compromise business security. Here are four:

First, *technology will do it all*. Technology has changed the world in which we live. It's already seeding the next industrial revolution, forcing businesses to transform how they operate. As they become more dependent on technology to function, so too do its executives assume technology's ability to handle everything. And, in parallel, business leaders take for granted other critical facets of security like confidentiality, integrity, and availability. Often the aspect of security least valued is people. The COVID-19 crisis, however, has highlighted some of the dangers of this mindset. Two examples will suffice.

Example number one: patient health information. In the United States, HIPAA legislation meant that the medical profession could not use Skype, as it could potentially expose patient health information. With an estimated 1.67 billion people now using the video messaging platform, the sheer volume of numbers makes it a valuable target for information thieves. Nonetheless, while COVID-19 rages, doctors want you to use Skype and other digital technologies instead of going to see them in person (telemedicine). It's a smart workaround. But is it secure?

And so, we fall back on individuals. Have patients set up their home internet system with hard to break passwords? Have doctors' offices and hospitals built in extra security measures for their telecommunication routers?

Example number two: home-based working. Many companies' existing security plans are based on businesses operating out of physical locations from which the data risks can be quantified and managed. But ask the global professional workforce to go about their jobs from home and the threat landscape opens up considerably.

There is no system or process in place for this and, as businesses establish remote office working on the fly, they necessarily rely on individuals to be discerning about how they work. Easier said than done when personal distractions about health, job security, friends, and family may cause some to click on the phishing emails that have proliferated since COVID-19 began to claim global attention.

The second unhelpful assumption being made is that *business continuity plans are the way to secure the enterprise in times of crisis*. Typical continuity plans are based on one-off, time-bound threats. After 9/11, for example, several trading firms working out of Manhattan established emergency premises in New Jersey to which they could decamp in the event of a similar disaster. Other companies too create business continuity plans based on localized, short-lived events like fires or hurricanes, with outages of 30 to 60 days expected.

In all instances, the plan assumes a discrete situation followed by a clean-up and carry-on approach. Very few businesses, if any, have a set of actions in place they know to take that has built into it an ongoing outage of unquantifiable time horizons.

The point is that you cannot always rely on continuity plans to see your enterprise through in a secure way. Situations like this call upon the agility and resilience of a business's people and the extent to which, never mind everything else they have to worry about, they're able to be aware and proactive about security risks.

The third unhelpful assumption is that *corporate boards know how to steer the ship*. There's a whole mythology around boards of directors and the executive teams surrounding them. Sure, in most instances, they know what they're doing. But the truth is that business leaders are prone to many of the same human anxieties as those they lead. It's one thing to help a business navigate through waters that while new, have a basic familiarity about them. It's quite another when—as has been the case with COVID-19—something comes at the business community from deep left field.

All of which means at least two things. First, a board needs to be very clear about what constitutes its mission-critical data, resources, and systems. Second, it needs to be clear that it's everyone's job to protect it. So that, as boards spend entire days locked up in business recovery meetings, people across the enterprise continue to factor security into their day-job.

The fourth assumption being made about how business works that may in itself compromise business security is that *compliance with regulatory frameworks gives companies the safety they need*. Once upon a time, while perhaps seen as a tedious task, compliance with the law gave the business community a sense of surety. Now, however, it can no longer be an operating assumption that a company is protected because it is up to date with all its legal requirements.

For a start, a recent study from the Economist Intelligence Unit found that the speed of technological disruption is making it difficult for regulators to keep pace, and there is a need for more and more sensible regulation of technology to safeguard innovation and the benefits of today's connected society.

This means that the legal profession hasn't yet caught up with the contemporary business world's stage of connectedness. It's likely too that, ongoing, new regulations won't be able to keep up and completely address new challenges posed by exponentially advancing technology and its impact on society. Not only that but with global businesses operating across several geographies, few jurisdictions, if any, are the same in terms of their regulations, privacy legislation, fraud, and breach prevention.

Despite early attempts to pass significant regulation, technology will continue to grow beyond the ability of any government to secure it; and a lack of international rules will be a wide-ranging cause for concern—with new and conflicting regulations causing strategic difficulties for many organizations. For example, laws intended to protect individual privacy will clash with those designed to make data processing more transparent. Identifying who holds blame and liability for security will become less clear.

*Technology will continue to grow beyond the ability of any government to secure it; and a lack of international rules will be a wide-ranging cause for concern.*

Nor does the lag in legal underpinnings mean the business community can ignore existing compliance requirements. There is no way to get around data privacy laws and regulations, even if they are not one hundred percent fit for purpose. Businesses must either conform or pay a steep penalty.

The bottom line is: while businesses ignore legal and regulatory frameworks at their peril, equally, executives shouldn't trust established, institutional wisdom to do their thinking for them.

Instead, they should consider an integrated approach to risk management and the discernment of the people in their businesses to put the right security protocols in place.

## Putting Security on the Corporate Radar

With the threat of cyber crime increasing and the operating environment becoming more complex it seems that the vital piece in the puzzle is your business's people and their smartness when it comes to security as an issue.

So, what is a business executive to do? What's the information he or she needs to safeguard the business he or she leads?

For one, not to assume he or she has timely access to all relevant information. And be aware of the fact that it may no longer be available.

In the face of the escalating global cyber related threats discussed in this essay, executives will need to be able to make methodical and extensive commitments to ensure that practical plans are in place to adapt to significant technological changes.

As we move forward, risk resilience must become a core aspect of enterprise risk management. This resilience must be built on a foundation of preparedness that evaluates the threat vectors from a position of business acceptability and risk profiling.

Enlightened organizations have now moved to a risk-based approach to managing cyber risk. The corporate organizations they lead understand that cyber is entirely embedded across the business. In other words, cyber risk is actually a threat to business as opposed to something that the technology department can manage. This awareness of total business vulnerability has been a reality check for many.

*The increasing complexities of the security challenge mean that the role of the security leader in the business environment needs to change.*

Gone too are the thoughts of throwing a security blanket over the entire enterprise—whatever that might look like. Instead, businesses need to embrace the need for alignment with a risk-based approach that reflects their respective risk appetites about the achievement of business key performance indicators that align with the delivery of their overall corporate strategies.

Organizations of all sizes will need to prepare thoroughly to deal with attacks on their valuable data and reputations. The faster leaders can respond to these problems, the better their businesses' outcomes will be.

## Security Quantification

The increasing complexities of the security challenge mean that the role of the security leader in the business environment needs to change. I already see many organizations getting ahead of the curve on this too, with executives working with their human resources experts to articulate the capabilities needed in their security and business functions. Plans are being made to upskill where possible or to hire in where not.

The point is for businesses to move away from behavior that's full of techno-babble and advice that's policing-centric. The smartest security professionals are able or are learning to use business-centric language, and to quantify security's return on investment. In scenarios where budgets are limited, as is highly likely in the post COVID-19 era, these skills will come into their own.

It's worth saying that, right now, technology vendors and tools overload the market for security. This leads potential employees to understand information security and compliance as profoundly technical. Recruiters can be left struggling to identify and appeal to candidates with a less traditional mix of education and experience. Nevertheless, smart organizations are swiftly recognizing that bright, diligent, curious individuals are among the most valuable assets an enterprise can leverage.

An approach to information security and compliance that thinks of people as people—rather than, say, a set of technical skills—will foster a workforce that can meet the challenges presented by digital risk.

Another point is that businesses, like governments, for that matter, need to start conceptualizing security as not just a technical function but as a whole enterprise concern.

> *Businesses, like governments, for that matter, need to start conceptualizing security as not just a technical function but as a whole enterprise concern.*

But it's not just the security team executives need to think about when it comes to the importance of people's roles in keeping an enterprise safe; companies should now take a 'people-first, technology second approach' and look to achieve a happy marriage of the two.

Senior business leaders too need to sharpen their skills. All executives, not just the board, need to be *au fait* with the challenge of cyber. Again, it must not be allowed to be seen as a marginalized activity that's part of the technology department's brief. Organizations that fail to adopt a more creative approach will find themselves dangerously shorthanded in the next few years, as both attacks and defensive measures become more complex.

Adopting a resilience-based approach to cyber security is also important. Cyber resilience requires the recognition that organizations must prepare now to deal with severe impacts from cyber threats that cannot be predicted or prevented. This in turn requires a high degree of partnering and collaboration both across the organization and outside with industry bodies, law enforcement, and like-minded businesses. This must be coupled with an ability across the organization to prevent, detect, and respond quickly and effectively—not just to incidents, but also to the consequences of such incidents.

This will require four key things to be put in place:

- *sound governance*: the organization will need to have an effective governance framework for monitoring cyber activities, including collaboration with partners, along with specific risks and obligations incurred through operating in cyber;
- *situational awareness*: a process, tried and tested, for gathering, analyzing, and sharing cyber intelligence;
- *resilience assessment*: a process for assessing and adjusting resilience to the impacts from the past, present, and future cyber activity; and
- *response*: the organization should be capable of preventing or at least detecting and responding to cyber incidents in order to minimize their impacts on the business.

For some, the above may already be well on the road to implementation. For others, this will be new and may require a focus and alignment of cooperation and collaboration across the business and its necessary stakeholders.

## Preparation Begins Now

As data breaches increase, new technologies emerge, and the geopolitical landscape becomes more complex, business leaders need to rethink cyber. Increasingly they need to view it, not as some sci-fi, other-worldly phenomenon best left to the technical folks, but as one that, left unguarded, can wreak significant, concrete damage. By this I mean in substantial negative economic impacts and damage to brand reputation, the latter of which can, of itself, affect a business's perceived and financial markets value.

The organizations that are able to see security as a strategic business issue—one in which people throughout the enterprise have a role to play—will be the ones that will thrive in the time ahead.

Attackers will continue to be presented with the tools and opportunities to target and exploit those who are unprepared. When digital and physical worlds collide, only organizations that take decisive action will thrive.