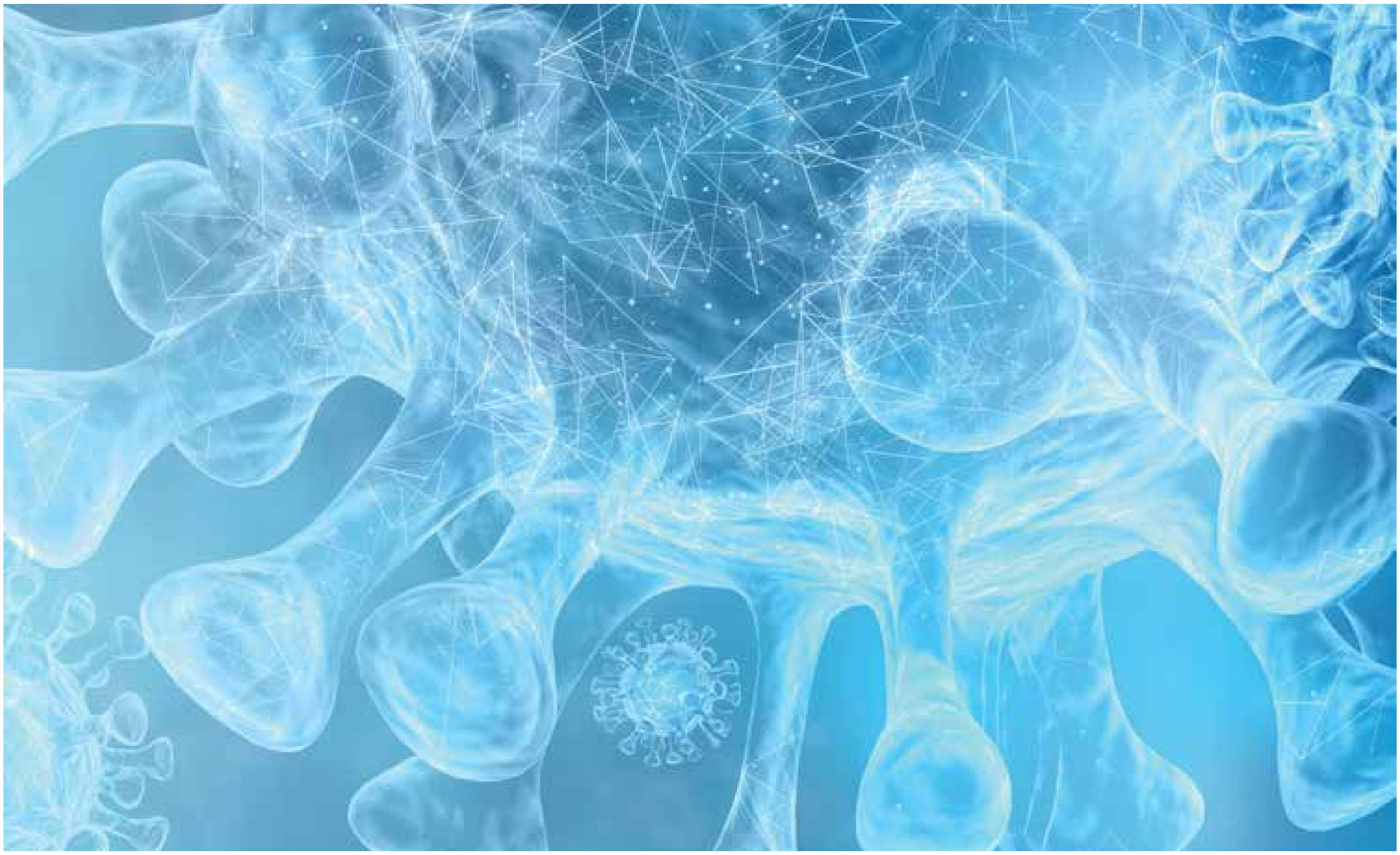


The Pandemic Is a Catalyst for Better Board Discussions About Cybersecurity

By Mike Lloyd and Ray Rothrock

Cybersecurity is a universal challenge because there is an appreciable part of every modern organization's business that is digital and therefore vulnerable to cyberattack. And this really is a war, albeit with blurred front lines and unclear rules of engagement. But the perennial challenge for directors is to clear away the fog. The cyber landscape is exceptionally difficult because it is constantly shifting—and winning depends on those who can best act on imperfect information.

In this context, any common language or shared concepts about risk control should be seized as a tool for leadership, to build common understanding and drive coordinated action. This is why the current global pandemic is a useful framework—the analogy between cyber risks and health risks has a great deal to teach us. It can be a catalyst for better board-level discussions about managing cyber risk and becoming more digitally resilient.

THE BIG LESSONS OF THE PANDEMIC

"Pan" means everywhere and everyone. COVID-19 isn't some arcane new business jargon, understood only by an elite priesthood of consultants. Everyone in your organization has been forced to learn about viruses and the impacts they have. This is part of what makes the pandemic so useful as an analogy and a tool for building a shared understanding of cybersecurity best practices.

Three clear imperatives of our new everyday lives have been hammered home by public health officials, scientists, and government leaders: social distancing, contact tracing, and basic hygiene.

Each of these imperatives has a direct parallel in network security that can give people a tangible way to relate common experience to some quite abstract-sounding problems in cyber defense.

MINIMIZE RISKY CONNECTIONS

More than anything else, public health advice through the pandemic has made people aware of how interconnected we are—through handshakes, shared surfaces we touch, even shared air that we breathe. What used to be easy to ignore is suddenly front and center, with people realizing the risks inherent in things as routine as catching a flight or working in an office. This same shift of mindset is necessary for digital life. What we start out thinking of as routine and beneficial is indeed both of those things, but also carries risk. We need to accept that everything online is vulnerable to a greater or lesser extent.

APPLYING BASIC PRACTICES IN A RIGOROUS, CONSISTENT WAY CAN YIELD HUGE BENEFITS, EVEN AGAINST AN UNSEEN AND INSCRUTABLE ENEMY.

Years ago, networks were built like medieval cities, with stout border walls and a carefully controlled gateway called a firewall, but there was little protection once you were inside the barriers. However, in our daily lives, we no longer live in these walled cities. Why not? Essentially, cannons became too powerful. We also began using less easily stolen forms of wealth such as shared credit in account books, rather than herds of cattle or gold bars. Our daily lives had to adapt. Instead of relying on the city wall, we had to learn to live in more fluid environments. This is comparable to changes in modern business networks as they migrate onto the cloud, breaking down traditional borders. But these changes haven't created a free-for-all. They've brought about initiatives such as micro-segmentation, which is essentially social distancing for computers.

Maintaining social distance is important during the pandemic because it can slow the spread of the virus, which tries to exploit our social interactions. Likewise, cyberattackers try to exploit the free connectivity pathways in our networks, spreading from computer to computer and hoping to remain unseen in much the same way that a virus does; it's no coincidence that one of the first online threats was dubbed a computer virus. As humans facing a pandemic, we've all had to think seriously about how to limit physical contact with others—in grocery stores, taxis, and more. We've had to reexamine how we do the things we enjoy, realizing that some precautions are necessary so that our recreation doesn't cause excessive risk.

The same trade-off happens online—your company network with its connections to customers and suppliers exists so you can do business, but these connections open potential pathways for attack. Some of your organization's assets must be separated from the outside world or your business risks attracting online viruses, ransomware, or bad actors. It's not easy to apply social distancing to your network and maintain it, but your network will be healthier for it.

HUNT AND TRACE

Contact tracing is a relatively new term that everyone has had to learn. We know we can't just put up walls, isolate our neighborhoods, our cities, or even our country, and assume no more infected people will come in or go out. That's not realistic in today's interconnected world. Instead, we have to assume that infection will arrive and be ready to track it down and stop its spread using contact tracing. These principles apply to modern business networks for the same reasons. You should invest in solid security controls, but still assume they will be subverted. Businesses therefore need a way to sense and track down the inevitable incursions. In cyber jargon, this is often called "threat hunting."

In both the pandemic and the virtual environment, it takes a combination of people and technology to perform such tracing efforts—first to find outbreaks, and then to track down where the spread has occurred. The situations aren't completely identical. People who get sick often self-identify by visiting a doctor, triggering the question of who else they had contact with. Computers that have been compromised do not give up this important information so easily. But to balance this disadvantage, the network of connections between computers, while large and complex, is much easier to map out completely than the network of all human interactions. So the imperative for directors and security teams is to invest in readiness planning—a combination of technology to map out business flows and normal activity, and people who can sleuth out the subtle ways that attackers attempt to hide their tracks as they move around.

An investment in virtual contact tracing has a significant secondary advantage, too. Digital business has a natural wildness to it due to the rapid pace of change and the human tendency to make mistakes and lose track of details. The threat-hunting teams that become expert in mapping out and scouting the hills and valleys of your online business are a great resource for gathering dispersed tribal knowledge, understanding how your business really works. This can pay dividends in readiness of other types, such as natural disaster planning or even audit planning.

WASH, RINSE, REPEAT

Finally, and most important, if there's one message that has been drummed into people about the pandemic, it's that basic hygiene really matters. While we wait for medical breakthroughs, we can slow down and even stop this virus if we increase compliance with the most basic rules: wash your hands and wear a mask. This can flatten the curve, directly saving lives in the process and possibly even turning the tide of the pandemic.

Sadly, it's been difficult to get people to internalize this message. There's a tendency to think, I've never had to take these precautions before, so are they really necessary now? People have a hard time adjusting to a world in which colleagues, friends, and loved ones can all be a threat. The virus is sneaky—it doesn't telegraph its presence until days or even weeks after it first infects someone, and consequently, people unwittingly take risks.

This inconvenient but necessary change of mind-set in cybersecurity is called "zero trust." This can be a misleading label—nobody who has ever walked into a building truly practices zero trust. No matter how professionally paranoid we believe ourselves to be, we trust that the building will remain standing. Still, the message is clear: don't assume the perimeter wall will save you, don't assume a network endpoint is OK just because it was OK yesterday, and always, always practice basic online hygiene—for example, report suspected phishing emails and require periodic security training for all employees.

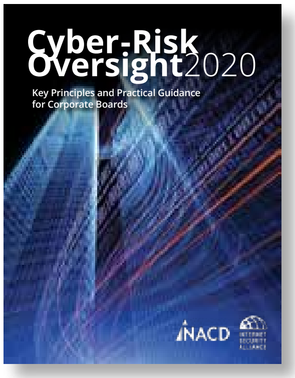
One unexpected parallel between cybersecurity and the pandemic is how effective these fundamental practices are. We tend to assume that complex problems need equally complex solutions, but that isn't true. Often, applying basic practices in a rigorous, consistent way can yield huge benefits, even against an unseen and inscrutable enemy.

In security, we must adhere to fundamentals. Too many intrusions are allowed by simple oversights. Sadly, our networks don't have sophisticated immune systems the way our bodies do. Our immune systems are capable of blocking and eliminating all kinds of threats automatically and it takes something new, such as COVID-19, to overwhelm our biological defenses. In our virtual networks, though, we haven't had the benefit of millions of years of evolution. There are pioneering researchers trying to build up the immune response of computer networks, but it's no easy feat to replicate the machinery that makes up human bodies. As your business becomes more digital, gaining the benefits of agility and scale, it also becomes significantly more fragile and prone to falling victim to whatever new digital pathogens come along.

As corporate directors, you are responsible for overseeing this complex and growing vulnerability. This means that you need to ensure every corner of your digital business is mapped out and inventoried and that everything is set up securely. Demand compliance with standardized rules for how networks are set up and maintained. These are policies established by industries, governments, and your own organization. Then, the extent to which the rules are being followed should be measured and reported.

THE NACD FRAMEWORK

The *NACD Director's Handbook on Cyber-Risk Oversight* was published in February 2020. The five-point framework contained within is a solid launch point for effective risk management, and the guidance expounds on the lessons from the pandemic detailed here.


Cyber-Risk Oversight2020
Key Principles and Practical Guidance for Corporate Boards
NACD
INTERNET SECURITY ALLIANCE

Public health officials need to coordinate regional and national strategy for the pandemic, calling in necessary expertise and tracking what is happening with robust reporting programs. Corporate directors need to manage cybersecurity in the same ways—applying oversight, coordinating plans, attending to legal ramifications, and above all, monitoring the real security situation using understandable reporting on real digital resilience.

In essence, the framework clarifies the need to get past the gobbledygook of typical security updates to focus instead on simple, repeatable measurements that capture the people, process, and technology that make up your security strategy.

THE COMPARISONS CONTINUE

Our experience shows us that the points of comparison between cybersecurity best practices and the pandemic can bring a great deal of insight. Digital acceleration has forced every business to understand security concepts that didn't exist a couple of years ago, just as individuals across the globe have been forced to understand new concepts and change their habits for their own health and safety through the pandemic. In essence, companies and individuals alike must learn the disciplines of social or asset distancing, threat hunting or contact tracing, and, above all else, basic hygiene.

In both a pandemic and network security, we need to help ourselves. Hoping that the next magical technology solution from a security vendor is going to make all business ills disappear is similar to waiting for a cure-all pill. The complexities of human biology are not going away anytime soon, and neither is the comparable complexity of digital business.

Mike Lloyd is an epidemiologist-turned-chief technology officer of RedSeal. Ray Rothrock is the executive chair of RedSeal, the author of *Digital Resilience: Is Your Company Ready for the Next Cyber Threat?*, and serves on the board of the NACD Northern California Chapter.