McKinsey&Company

Staying ahead on cyber security

January 2017

Is your company an easy target for hackers? Even those making progress must keep moving to protect their digital assets.

As digitization accelerates, it's critical for organizations to shore up their defenses to ensure information systems are well protected. But with threats on all sides, where should companies begin, and how do they keep pace with constant shifts in the landscape? In this episode of the *McKinsey Podcast,* leaders of McKinsey's Cyber Solutions, VP Dayne Myers and consultant Marc Sorel, speak with McKinsey Publishing's Simon London about ways to manage cyber security risk, build digital resilience, prioritize critical assets, and embrace a broad, business-wide perspective—even if your plan isn't perfect.

Podcast transcript

Simon London: Hello, and welcome to this edition of the *McKinsey Podcast.* I'm Simon London, an editor with McKinsey Publishing. Today, we're going to be talking about cyber security, how organizations can deal with the increasingly sophisticated threats to their information systems and assets. Joining me here in our Silicon Valley office to discuss the issues are Dayne Myers and Marc Sorel, leaders of McKinsey's Cyber Solutions. Dayne and Marc, thank you very much for being here today.

Dayne Myers: Thank you for having us.

Simon London: A year ago, we had our wonderful colleague, James Kaplan, on this podcast. We talked about some of the fundamentals of cyber security. He also introduced the concept of digital resilience, which I think we'll go into in more detail later. But before we do that, just look back on 2016, a year since James was on here talking about cyber security. How did the year shape up in the end?

Dayne Myers: Well, Simon, I would say that one of the most significant things we're seeing is that cyber security risk in particular is much more becoming a board issue. Boards of directors are feeling like they need to pay attention to this.

I think another thing we've learned is that a lot of boards and CEOs are becoming more concerned about the money they are spending and whether or not they are getting adequate return on their investment in cyber security technology and defenses, and also whether or not they are prioritizing the right things.

One final point is that, as the world gets more digitized, as companies of all sorts—not just cloud-based companies and not just software companies—are becoming more digitized, that threat goes up exponentially. And innovation is slowed, obviously, if you're attacked. But also trying to plan out cyber security in a way that does not slow down that digitization and that innovation is difficult.

Simon London: Something that James mentioned last year was some initial data we had showing that among cyber security professionals, there was a feeling that the attackers were moving faster and innovating faster than the good guys. Is that still the case?

Marc Sorel: Absolutely it is, Simon. And I think actually we've seen an acceleration of that gap growth between the attackers and the defenders. You can look at it any number of ways, but probably the best way is in terms of time to exfiltrate against time to quarantine.

Time to exfiltrate is how fast it takes me to get in and get what I'm after if I'm an attacker. Time to quarantine is how long it takes me to stop you once I know you're there. If you very simply look at those as two line graphs, in terms of what the time is, the gap between them is getting broader in favor of the attackers.

We've definitely seen that. And I wanted to return briefly to something Dayne was saying about what happened in the last year. A more direct line is being drawn between value and value creation and the impact of cyber security attacks and hacks and breaches. We're also seeing this question arise more and more in private-equity firms that we're serving. Both pre-acquisition and post-acquisition, they are asking about the red flags to worry about from a capex and opex perspective on the security side—the things that, if I don't take care of them today, are going to get in the way of my ability to devote dollars to digital strategy and get the private-equity returns that I want.

Simon London: Something else about 2016, if you read the newspapers, whether it's real or suspected, is hacking by state-sponsored actors. That seems to be something that, at least in the popular imagination, has become more prominent. Is that something companies are worrying about more and having to worry about more on the ground?

Marc Sorel: The concern we're hearing from companies is, I think, less focused on nation-states. There's an understanding by companies that just because it's in the headlines doesn't necessarily mean it's a new trend or something that is increasing. It could just be something that has always been there but is being more prominently exposed. A lot of the companies we work with understand that. What they're more focused on is the analysis around actors and vectors.

So who are the most likely actors? What are the most likely vectors? Of course, there are going to be certain ones for certain reasons that are attractive to nation-state actors. But in most cases, most companies will be most attractive to nonstate or semistate actors. I'm talking about criminal syndicates or associated groups of hackers that may not have a nation-state affiliation. And typically in terms of vector, they are using very conventional channels for attack, like phishing.

It's important to remember that the real day-to-day risk out there is something much more simple and basic, like phishing, which drives 80 to 90 percent of attack volumes today. And it will continue to. The attackers that are following on that still are those syndicates, or groups of attackers, and even your own employees, wittingly and unwittingly, rather than those sorts of very sophisticated nation-state actors.

Dayne Myers: As Marc mentioned, the nation-states got a lot of attention due to the election cycle. And the news was about the nation-states, but it varies from nation-states to organized crime. You can even go on the dark web and find a black market for attack code.

For as little as $150, anybody can go buy code that is very effective at hacking. Effectively, this has commoditized the market for attack software, which is the armament of hacking. As a result, you've got this range all the way from nation-states that are developing cyber weapons, all the way down to individuals who can go on the dark web and, with some Bitcoins, buy attack code and be untraceable.

You have to be prepared for the entire spectrum. No matter what you hear in the news, all of it is happening, and you have to be prepared for all of it. It's not even about being perfectly defended against all of these threats. It's about managing the risk and managing the threat as best you can.

Simon London: That implies that it's also not only the very large companies that are being targeted. I think we've seen this in the news as well with things like ransomware increasingly hitting relatively small ones, and certainly midsize companies. Is that right?

Marc Sorel: Absolutely. You can look at a lot of different data that will suggest, in a variety of industries and geographies, that the number of midmarket companies that are being attacked is growing. And the number of attacks being executed against them is growing.

In terms of your point about ransomware, we've also seen ransomware grow as a method. Just to give you some perspective on what ransomware is: it's basically where someone, potentially inside but usually outside of an organization, will go in and get access to the system, move around inside the enterprise environment, and then enact some kind of code or capability that will prevent the company in question from accessing that part of their systems. And then the attacker will ask for a ransom to unlock that system, or rerelease the data that they've quarantined from the company's access.

One great example of this was what happened with Hollywood Presbyterian Medical Center, where there was a ransomware attack against their systems. And most recently it happened with the San Francisco Municipal Transportation Agency. For all of these, the ransomware attackers actually asked for a ransom in Bitcoin. Usually it's a pretty small sum, somewhere below $100,000. So not quite the direct impact you would expect in terms of magnitude of value at stake. But in terms of downtime, in terms of reputational risk, in terms of brand risk, and then subsequent top-line revenue coming out with your operations, it can be a pretty substantial impact on the business.

Dayne Myers: One more thing to add to that: the way attackers look to things has shifted. They used to look at where there is a lot of money, where to go find a lot of money. [But now it's] where is the weakest victim?

They're not going to bother with somebody that's very well protected. Nobody's going to be perfectly protected. It's really about just staying better protected than others, being less of a target, and being less exposed. Because the attackers are going to go where it's easiest to hit now. It's not necessarily just where there's the most money.

Simon London: That's a lovely segue into the question of what you do about, obviously, the way the threat landscape is getting more complex. It's getting more dangerous out there, if anything. James introduced this concept of digital resilience.

What have we learned about the habits of digitally resilient enterprises? What are some of the things we see out there that the more mature, more resilient enterprises do?

Marc Sorel: Simon, there are a few things that we see. And just to refresh the concept of digital resilience, it's a seven-section framework that we developed in work with the World Economic Forum and a variety of business-executive and technical leads around the world.

It basically talks about not just the technical side of cyber security but also the governance and the business side of cyber security. To give you some examples of the elements that are in that seven-piece framework, things not just like how you build security in your technology environment, but how do you think about making sure that new applications you develop are secure? Also, how do you think about the governance of cyber security? Are you reporting on the topic to your board? If so, how frequently, and who's having the conversation?

What we found in our work with the Digital Resilience Assessment, which now has served over 70 companies and, through a variety of sources, brings together a perspective of assessments conducted against over 200 companies, as well as a database of many more companies than that to benchmark performance in terms of security and maturity—we basically put together the results of that to find a couple conclusions. One of the main takeaways for us from the work is that digitally resilient companies are ones that have figured out security matters enough to create a leadership position at the C-level dedicated to the task.

This usually is in the form of a chief information-security officer. The companies that have that type of position in place tend to score overall across the seven dimensions about 25 to 40 percent better than their peers that do not have such a role in place.

What we also found is that—and this is probably more an outcome of a lot of other factors—companies that have a regular board-reporting cadence on cyber security also tend to score better. Usually that's not necessarily just because they're reporting to the board but because they have in place the systems of controls, the systems of data analysis. They also have the capabilities to make this something that (a) you feel comfortable taking in front of the board and (b) you know well enough to speak about with the board in a way that's plain English that they can understand. While that may not be the

driver of the maturity, it is a good indicator of maturity and digital resilience at a company.

Simon London: The other thing that I noticed, looking through the recent research, is companies that use realistic simulations—war-gaming, basically—tend to have higher scores on resilience and maturity. Is that right?

Marc Sorel: Yes, it is. And there, they scored on average about 30 to 40 percent higher than their peers as well. So just to give you a concrete example of one incidence where we served a private-equity firm on this topic. We actually helped them to design an end-to-end incident-response simulation over a four-hour period, when we actually delivered it, that included their senior-executive team and their technical team.

The simulation included a variety of scenarios they had to grapple with where we talked about different compromises of sensitive client data, as well as investor-related data that they then had to address in their work with both their clients as well as their portfolio companies. What we discovered from that simulation was even though in the first hour there was report of a significant compromise of sensitive data on a key server in their environment, it wasn't until hour three that they asked whether or not they should be contacting the regulatory authorities.

When that question finally got asked, there was this pause in the room where everyone realized, "Gosh, first of all, we should've asked that question at the start. And second of all, do we even understand when a situation rises to the level of consequence that it would require us to reach out?" One of the main recognitions from that first exercise, which we find for more mature companies that have done it many times, is that, actually, before the crisis occurs, you can already have in place the controls and guidelines you need to know how to decide 70 to 80 percent of the difficult decisions you'll have to take under that crisis setting. Just the act and practice of putting into place those capabilities already significantly moves you down the path toward greater maturity and security.

Simon London: It's interesting that you said there, Marc, that the simulations and war games are something that you should be doing annually, for example. And it sounds like a lot of this is not a one-and-done thing, right?

Dayne Myers: I think that's exactly right. It doesn't matter where an organization is on the spectrum of cybermaturity. It's a matter of basic hygiene. It's almost like the equivalent of dental brushing and flossing. Even if you aren't doing it regularly enough, you have to start, and you have to do it regularly.

It doesn't matter whether you're mature on that standpoint and you've always been doing it. You still have to keep doing it. You still have to keep improving. You still have to keep staying on top of things. If you're less mature, you have to get started.

Marc Sorel: One example from our recent work involves a Fortune 100 consumer-goods manufacturer. The situation was that its chief information-security officer was struggling to get his security program off the ground.

He had come recently from another employer and knew that the consumer-goods manufacturer was behind. But he hadn't yet been effective in rallying the troops. We came in to do some work with him and conduct the initial Digital Resilience Assessment, which does this top-down benchmarking to peers.

From the findings that we came away with, it became quite clear there were a couple places where the company needed to act and needed to act quickly. Number one was to identify what the critical assets were in the environment. Because you can't conduct good incident-response simulations, you can't prioritize your spend, and you can't properly secure yourself against threats without knowing what you have and what matters.

Simon London: This is the "crown jewels" concept, right?

Marc Sorel: Exactly. The other things that we discovered were that it didn't really have that incident-response-simulation muscle memory that we were talking about. The company needed to build it quickly, partly because, as a consumer-goods manufacturer, it had a very much consumer-facing part of the business that, over the next five years, it was looking to grow in a way that would be more consumer focused, direct to consumer, and digital. The threat landscape was growing because of the new capabilities the company was bringing on board. After the incident-response simulation and the critical-assets identification, there was also an implication for how to think about structuring the information-security organization.

Because, at the present time, security was the responsibility of many people part-time instead of a few people full-time. Consequently, it just wasn't getting the attention that it needed and deserved, especially in things like upstream application development for some of the digital tools that the business wanted to create. Therefore, it risked creating a lot of slowdown in time to market.

The last piece that came out of this was that it had a franchise group that it was working with. Basically, that group also was interacting with its digital systems. It was unclear with these third parties what exactly their threat exposure was. What it also needed to do was figure out what the third-party risk was—not just how to structure the organization, build its response capability, or prioritize its assets.

Over the past year, coming out of that assessment work, we've been working very closely with it across many of these steps in the journey to help it get to where it needs to be, not just to be secure but also to use security as a method and means for enabling the business going forward.

Simon London: Can we go back to this concept of crown jewels? It's easy to say that, of course, you should prioritize those assets and systems that are most business critical. But I would imagine that, in practice, if you're a large enterprise, that's actually a nontrivial piece of work to figure out what the assets are: who owns them internally, what the governance is, how to protect them.

Marc Sorel: It is very hard work. And it's work that is time consuming, Simon. How that typically works in practice and how we think about approaching it is that a firm will typically

look at, first, how do my systems and assets map to each other? That's really where the hard work begins. Our cyberrisk-insights solution helps companies looking to do that hard work by starting with a 60 percent solution.

Over a period of five to eight weeks on an individual business-unit basis, companies will try to basically richly map their systems to their assets, to their threat landscape, to their business value chain. Based on that, they prioritize their assets and say, "OK, what are the controls we ought to have in place versus what we have in place today? And then what's our plan to close the control gaps over time?" That's the hard work.

Dayne Myers: And to what Marc said, I'd add that the fact is that a step a lot of companies need to take now is they do some of these things at an IT level, but they don't involve the business perspective on the risks.

It's one thing to take an IT perspective. But that's generally not sufficient to really understand and manage the risk. You need that business perspective. We've been advising companies to make that leap to make it more of a business issue, not just a tech issue, and to look at the tech within the ecosystem of the business as a whole.

Marc Sorel: There are different contexts and frames in which this risk management is going to need to be applied. It's not just about conventional IT anymore.

As you think about the Internet of Things and specifically operational technology, where you have next-horizon environments for threats, there are a couple of factors to keep in mind.

One is just the sheer explosion of connectivity devices and persistence in the technology environment. What I mean by those things is you have more people touching more objects. Those objects are communicating with each other more often and more regularly. That's creating a volume of communication and code and data that is transited from many points to many points at a degree of complexity that no single institution or person can track.

That's creating a lot more risk in terms of the threat landscape. I'll give you a couple of examples. One recent example we had was talking with a utility that was looking to get help on cyber security. For a utility, of course, you have both a very robust IT environment, but also OT, your operational technology. Specifically, that means things like the industrial-control systems you might have in place in a water-filtration plant that tell you when to filter the water and how. If that gets compromised, of course it can have significant repercussions for the population it serves.

One of the key risks there is that OT historically has been treated very differently from IT in terms of how it gets updated. Information technology gets patched and updated regularly. Think about the OS on your iPhone. You're constantly getting a new version that you just point and click to get. OT is updated on a multiyear basis. When things are updating at a different pace, there's going to start to be daylight in terms of how they work, and therefore how you can exploit them. That creates situations like what we saw with a dam that was hacked by a hacker who got in through a front-end payment processor. Or [there was] a water-filtration plant elsewhere in the US that got hacked and actually had the chemical composition of its water altered.

Another area to get interested in and excited about is cloud security. If you think about the migration to cloud happening today, the number-one reason we find through McKinsey's enterprise cloud survey as to why companies don't migrate to cloud is security concerns.

They're just not sure how to think about securing everything they would like to move to the cloud, despite the benefits cloud might confer on their business in terms of taking cost out. In all of these areas, cyber security's going to play an increasingly important role. I think it will be a place where there is a lot of impact that can be driven for people who can get the answer right about how you think about security as an integral part of your business.

Simon London: And, to your point, Dayne, this speaks to that tension between innovation and security. There's a constant push and pull there, and, I would guess, quite a lot of tension between security experts and business units: people who want to do things and people who are advising them to take it slowly.

Dayne Myers: That's a very good point. On top of that, this goes back to the issue we discussed earlier about getting business executives to buy in. We've been trying to help our clients understand and make that shift from IT security as really just a control function or a restriction on their ability to act that slows them down. Rather, it is a continuous risk-management process that they need to build into their way of thinking and into their way of operating. Those companies that make that shift are the ones that are riding the wave better than the ones who are getting left behind.

Simon London: OK. Well, thank you very much. I think that's all we have time for today. But, Dayne and Marc, thanks for being here. To find out more about our work on cyber security and other issues, go to McKinsey.com. □

Dayne Myers is a Solution VP in McKinsey's Silicon Valley office, and **Marc Sorel** is a consultant in the Washington, DC, office. **Simon London** is a member of McKinsey Publishing and is based in the Silicon Valley office.