IronNet

The 7 Cs for CISOs

to communicate to their Board

Venture capitalists, cybersecurity leaders, and military experts weigh in on how to make a stronger business case for cybersecurity

The 7 Cs for CISOs
to communicate to their Board

1 | Core to business growth

2 | Challenging nation-state threats

3 | Competitive edge

4 | Collaborative threat intelligence

5 | Capabilities assessment

6 | Cyber talent shortage

7 | Credentials across the supply chain

Economic security is overall security.

Ted Schlein, *Partner at Kleiner Perkins*

Although cybersecurity has gained a more regular place at the Board table over recent years, we know that,

61% **OF DIRECTORS DON'T BELIEVE THAT CYBERSECURITY SHOULD GET IN THE WAY OF BUSINESS OPERATIONS.[1]**

In other words, it is common to prioritize business objectives over cybersecurity.

As CISOs experience firsthand, this traditional mindset has two fundamental problems:

1. It does not level up the need for strategic cybersecurity investment.
2. It suggests a failure of regarding cybersecurity as an inherent aspect of business strategy and growth.

Within this context, as you work to communicate your cybersecurity strategy to your Board, consider these "7 Cs of CISO Communication" to build rationale for advancing your planning and prioritization efforts. These insights come directly from IronNet Cybersecurity's own Board members.

1. 2019-2020 NACD Public Company Governance Survey, https://corpgov.law.harvard.edu/wp-content/uploads/2020/01/2019-2020-Public-Company-Survey.pdf

1. Core to business growth

Your role as cyber executives is to ensure the overall company is safe and secure. Security always needs to be talked about as core tech. As you are building your company and your business, you have to think about how you are going to build in cybersecurity as the essence of what you do.

Ted Schlein, *Partner at Kleiner Perkins*

Communicate that cybersecurity equals business strategy.

As you approach your Board, you may be up against the traditional assumption that cybersecurity is a cost center weighing on the bottom line. While this viewpoint is shifting quickly as digital transformation accelerates, continue to position cybersecurity as a strategic investment. Key to this change in thinking is the mantra that cyber risk goes well beyond IT.

The SolarWinds/SUNBURST and Microsoft Exchange server attacks are cases in point that should have every Board rethinking its approach to cybersecurity investment. In addition to the elite Russian adversaries in the SolarWinds case, highly sophisticated hackers worldwide are on a relentless mission. They're teaming up to launch coordinated, targeted, and damaging cyber attacks across the global digital landscape.

What are the results? An increase of cyber threats to business continuity and reputation, widespread attacks on supply chains, and the erosion of trust among both consumers and B2B customers.

Communicate the company's cyber risk in this context, along with measurable outcomes for lessening that risk, to strengthen your business rationale. In some cases, you may have to position "cyber risk" within either a "digital risk" or "business risk" framework to ensure cybersecurity has a seat at the table.

Hear more from Ted Schlein about positioning cybersecurity as business strategy in the on-demand webinar:

"Why cybersecurity isn't a post-pandemic luxury" >

Learn how to implement the strategy in the "10-step Executive Action Plan to Collective Defense" eBook.

Read more >

2. Challenging nation-state threats

> Cyber becomes such a useful and economic weapon for nation-state adversaries to use in the sense that it does not cost them what it takes to build a robust military yet they can get similar effects. This is one reason why it has exploded so much: they are operating below the level of conflict without the international risk … yet the gains are significant.

General (Ret.) Jack Keane, *Chairman, ISW, Former Vice Chief of Staff, U.S. Army*

Illustrate the rise of nation-state threats.

More pervasive and dangerous nation-state cyber threats are amplifying cyber risk considerations for companies and organizations, especially as digital transformation widens the attack surface and supply chains expand. Communicating these ongoing cyber threats, with concrete use cases, shines the light on the need to elevate cybersecurity investment as an inherent part of business strategy.

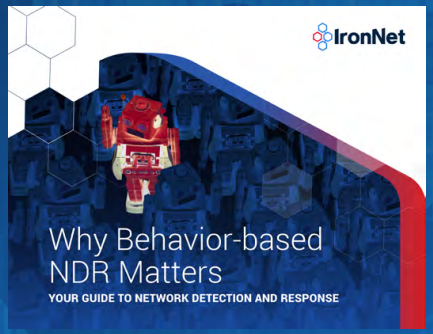
Who are the ones to watch and what are the threats? In addition to highly organized cyber criminal groups, nation-state adversaries to look out for include the big four: China, Russia, Iran, and North Korea. Recent Russian threats, for example, include the widespread SolarWinds/SUNBURST hack, and China is presumed to have carried out the widespread Microsoft Exchange server attack.

Raising an alarm to your Board about these significant threats must go hand in hand with communicating your capabilities for defending against them, as explored in #5: Capabilities assessment. As Vice Admiral (Ret.) Mike McConnell, Former Director of the NSA, emphasizes, "If we don't find a way to protect our intellectual property and creativity, China will outstrip us. We have to stop this outflow of intellectual property. If we do not, we will find ourselves at a very strong disadvantage in 10-12 years."

Hear more from General (Ret.) Jack Keane about the nation-state cyber threat landscape in the on-demand webinar:

"The next four years ... in cyber" >

Discover how a network detection and response system can be used as a defensive weapon against these nation-state actors and organized crime groups.



See the eBook >

3. Competitive edge

With Collective Defense, all data that flows anonymously through participating hospitals and clinics is analyzed in real-time to search for suspicious activity. Whenever a suspicious threat is detected, preventative action is taken across the network of hospitals, all the way down the supply chain, to block the attack before it occurs. This collaborative approach has completely changed the nature of cybersecurity at these hospitals.

André Pienaar, ***Founder of C5 Capital***

Emphasize security and digital transformation must go hand in hand.

Anticipating market needs, working fast, and pivoting quickly demand agility. The need for speed is clear. But, as the National Association of Corporate Directors observes, "Boards face a conundrum in balancing important cybersecurity concerns with continued pursuit of digital innovation, transformation, and ultimately corporate growth."

Security must be able to keep up with both innovation and digital transformation efforts; otherwise, all advancements could come to a screeching halt the moment your calling card to innovation and market differentiation — intellectual property — is stolen.

We can fight AI-driven cyber attacks with AI. As Jan Tighe, Retired Vice Admiral, Former Deputy Chief of Naval Operations for Information Warfare and Director, Naval Intelligence, U.S. Navy, says, "With AI involved in attacks, you have to speed the ability of SOC operators to identify threats and to deal with them. If you can see across the sector in other networks [with anonymized data], you can identify activities much more quickly than if you're seeing only your own data." Behavioral analytics based on machine learning can detect threats at network speed, well before they move to exploitation and exfiltration stages.

Draw on use cases, such as the aforementioned healthcare one by André Pienaar, and other sectors such as utilities, to make a case for building a security posture as agile and fast as digital transformation itself. The two must work in lockstep to maintain your competitive edge.

Hear more from André Pienaar about transformative cybersecurity in the on-demand webinar:

Funding resilience: A VC's view on the optimistic future of healthcare and cyber >

Find out how to detect threats as early as possible in the intrusion cycle, using behavioral analytics to see them "left of boom."

Access the white paper >

4. Collaborative threat intelligence

A collaborative approach between companies is the only way we are going to beat back these massive investments by nation-states and criminal groups on penetrating networks to steal intellectual property.

Mike Rogers, ***Former U.S. House Intelligence Committee Chairman and Vice Chairman of the Board of Trustees of MITRE Corporation***

Address concerns about data sharing and privacy.

Given the prevalence and sophistication of cyber threats, it is clear that no organization can keep up alone. What's more, the reality is that every company today operates as an extended enterprise dependent on an interconnected supply chain. If organizations keep operating individually in silos, no one will gain greater visibility of extensive supply chains and third-party networks.

Defending together depends on data sharing, and therein lies the elephant in the room: data privacy. Concerns about data privacy deter many companies from working collaboratively to defend as a unified front.

To make a case for collaborative threat intelligence, keep in mind that threat information-sharing in real time is anonymized. As Ted Schlein, Partner at Kleiner Perkins explains, "You can protect and share data at the same time. You don't need the specifics; you need the meta information because you're looking for patterns. Realizing that your safety and security are only as good as your other brethren in other industries is key. You have to defend in real-time."

Express to your Board that achieving visibility across sectors, made possible by threat-sharing at network speed within a Collective Defense platform, weakens adversaries as they attempt to move from one sector to the next (e.g., energy to finance), applying similar tactics, techniques, and procedures.

Hear more from Mike Rogers about the scale of threats that require data sharing to fight back in

Eyes only: Top U.S. and foreign cybersecurity policy issues >

Explore the myths surrounding data sharing in cybersecurity.

See the white paper >

5. Capabilities assessment

> One of the best practices I have seen in terms of educating directors and helping them understand their specific risk profile is having the CISO talk through the big breaches in the news most recently and walking the directors through the MITRE ATT&CK® Framework to explain how they happened and how prepared their company is to deal with that type of threat.

Jan Tighe, ***Retired Vice Admiral, Former Deputy Chief of Naval Operations for Information Warfare and Director, Naval Intelligence, US Navy***

Identify your weak spots and how to fix them.

Understanding the state of your cybersecurity controls is critical to your communication cause. As VIce Admiral (Ret.) Jan Tighe notes, “Some companies don’t know where to begin. If you don’t have a good sense of where your starting point is, it’s really hard to move forward. An option is to have a third party come in to do an assessment using the NIST Framework.” From there, turn to the MITRE ATT&CK® Framework to complement the common programmatic frameworks such as NIST as a way to determine the ability of your security capabilities to combat current cyber threats based on real-world observations.

Express to your Board that often the answer is not piling on more technology; instead, doing better can mean determining specific weak spots within the context of the MITRE ATT&CK® Framework. Learn how to do this in “5 practical ways for a CISO to use the MITRE ATT&CK® Framework”. The goal of this exercise is to identify where to prioritize investments in order to lessen risk as early as possible in the threat intrusion lifecycle.

This is how to build cyber resilience, that is, “the ability to defend against attacks while continuing to do 'business as usual' successfully” (Accenture). Capabilities must extend beyond traditional signature-based tools, endpoint protection, and firewalls as explained in IronNet’s network detection and response white paper. Indeed, reiterate that a traditional “castle and moat” approach to enterprise security is no longer sufficient, especially as supply chain security emerges as the biggest opportunity for threat actors to pounce and get into your network.

Hear more from Vice Admiral (Ret.) Jan Tighe about mapping cyber risk against capabilities in the on-demand webinar:

“From the top down: Why every board of directors needs to address cybersecurity >

Learn how to map your security capabilities against the MITRE ATT&CK® Framework to assess cyber risk.

Get the white paper >

6. Cyber talent shortage

> No one can afford the people they need to defend on the scale we need to, but imagine if you have 30 companies with three analysts each. You now have 90 people working on a common set of problems working together. That is the way to address the cyber skills shortage while also building stronger defense as a unified front.

General (Ret.) Keith Alexander, *Co-CEO of IronNet*

Suggest a way to improve security resources.

The cyber talent gap is a widespread challenge. The ratio of the volume of network traffic versus the number of cybersecurity specialists to analyze that traffic is severely lopsided. All organizations face a daily balancing act of staying steps ahead of hackers who constantly present risk to the global digital economy while the cyber talent gap grows wider every minute.

In short, your SOC analysts are overwhelmed. We all know the skills gap will continue to widen as network traffic proliferates. Capgemini reports that, "Global business internet traffic is expected to increase three-fold from 2017 to 2022." At the same time, the number of unfilled cybersecurity positions has surpassed four million worldwide. And guess what? Widespread 5G adoption is just around the corner. The human element of managing the growing and always-changing threat landscape is a deep concern.

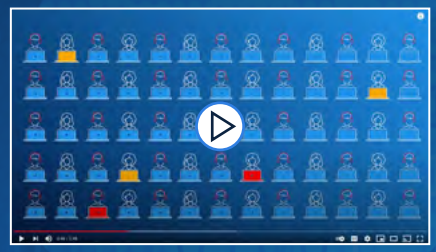
Communicate to your Board the need to improve the effectiveness of your security operations team. In many cases, this does not mean adding headcount. Either you can grow talent from within, as American Electric Power's Chief Security Officer advocates, or you can leverage the capabilities of other SOC teams through real-time information sharing, such as explained in "Your SOC. Multiplied."

Using the MITRE ATT&CK® Framework approach covered in #5, you can map out outcomes related to your team's performance in defending against observed threats. There is no need to get granular with your Board, but you can further build rationale for decision-making related to cybersecurity investments.

Hear more from General (Ret.) Keith Alexander on improving the capabilities of your SOC team in the on-demand webinar:

How to collaborate for a stronger cyber defense: Leadership advice from the front lines >

Watch how to multiply your SOC capabilities.



7. Credentials across the supply chain

> Most have not internalized that they are supply chain dependent. If people would just think about how dependent they are on the supply chain and then identify what is essential, it at least gives them a better perspective on how to address this set of issues. Thinking about how dependent we are on the supply chain and then identifying what is essential at least gives a better perspective on how to address this set of issues [e.g., intellectual property theft]. We need to take this issue seriously as an existential threat to the country.

Vice Admiral (Ret) Mike McConnell, *Former Director of the NSA*

Sound the alarm about securing the supply chain.

Nation-state adversaries are always on the move, hunting for the unguarded or most vulnerable links to exploit. They're looking to get in through back doors within vast, interconnected supply chain networks. According to Accenture Security, "Indirect attacks against weak links in the supply chain now account for 40 percent of security breaches." This is perhaps the most urgent message of all to convey to your Board.

In this context, ask the question, "How secure are the third-party entities my company relies on to conduct its business?" As companies shift from client-server environments to cloud and multi-cloud environments, they must be able to identify every entity operating across the supply chain.

"Identity is the new perimeter. We need to do a better job of identifying who is trying to get into the network," says ForgePoint Capital Co-Founder & Managing Director Don Dixon, in "The State of the Cybersecurity Market: Bull or Bear?"

Communicate the need to take a closer look at your supply chain security and more proactively managing third-party risk in the wake of more prevalent and bolder attempts by nation-state adversaries to infiltrate — and steal or compromise proprietary data — through the weak links. Other than perhaps phishing, the biggest area for hacks to be successful are via the people you allow to connect in to your network across the supply chain. Revisiting third-party risk is crucial.

Hear more from Vice Admiral (Ret.) Mike McConnell about protecting intellectual property in the on-demand webinar:

Why a national supply chain cybersecurity strategy matters >

Discover the most common supply chain attacks and how to prevent them in the "Securing the Supply Chain" white paper.

Read more >

There is no bigger problem that we have to solve than cybersecurity.

Don Dixon, *Co-Founder and Managing Director at ForgePoint Capital*

A major mind shift in cybersecurity is happening. As existential threats present challenges that are much greater than any single company or organization can manage alone, emphasize to your Board that now the time is now to defend together ... or get left behind.

Working with leading companies across sectors, IronNet has identified their shared cybersecurity pain points — and ways to solve them.

The Collective Defense platform, IronDome, empowers companies and organizations to stay ahead of evolving threats through real-time threat sharing and collaboration across industries and sectors. IronDefense Network Detection and Response, powered by advanced behavioral analytics, amplifies detection speed and efficacy, enabling quicker triage and faster response.

Hear more from Don Dixon on how leading companies are addressing the most pressing cybersecurity challenges in the on-demand webinar:

The State of the Cybersecurity Market: Bull or Bear? >

IronNet

To learn more, visit
IronNet.com