NordPass®

Build Your Defense From the Inside Out

10 tips for how to promote cybersecurity to your leadership team and colleagues

Foreword by NordPass CEO Jonas Karklys

IT leaders, this resource is for you.

The pressure to respond to the current cyber threat climate is daunting. To help, we invited three cybersecurity leaders for a discussion on the threat of cyberwarfare, its impact, and how businesses can defend themselves.

What we learned is that knowing which measures to take is only half the battle — the other is getting the right support for your program internally. That includes leadership signoff, budget, and buy-in from every member of the organization.

But given the barrage of cyber incidents in the headlines, businesses are now more primed to prioritize cybersecurity in 2022, increasing the likelihood of getting the green light for those much-needed protocols.

In this report, we've compiled the experts' best advice on how to make the most of those conversations with your team, for this quarter and beyond. With it, our goal is to empower you to get the support needed to safeguard your business and, ultimately, help you sleep more soundly.

Stay safe,

Jonas Karklys, CEO of NordPass and NordLocker, is a cybersecurity pioneer and co-founder of Nord Security—whose software products protect over 15 million people worldwide. Engaged in web-based projects since the age of 11, Jonas remains steadfast in his commitment to help create a radically better internet for everyone.

Table of Contents

1. Introduction

1.1 Meet the experts

Pete Gibson
CIO/CTO

Friendly's

Pete Gibson is a transformational technology executive with a track record for improving business, conducting major turnarounds, and innovative solutions. He has a record of success as CIO, CTO, and COO across different industries worldwide and, in those roles, has solved complex business problems by identifying and leveraging technologies, processes, and people. He has demonstrated a proven ability to implement systems and solutions that drive revenue and growth.

Sandy Dunn
CIO/CSO

BreachQuest

Sandy Dunn, CIO / CSO at BreachQuest has over 20 years' experience in cybersecurity. Initially starting out in software and hardware sales, she worked with NASA, JPL, the Secret Service, the IRS, and other federal agencies. Her roles in cybersecurity have included competitive intelligence, security engineer, information security officer, senior security strategist, IT security architect, and CISO. She prioritizes a risk-based, business-focused, strategic approach to cybersecurity through process, standards, and threat intelligence.

Alyssa Miller
BISO

S&P Global Ratings

Alyssa Miller, business information security officer (BISO) for S&P Global Ratings, directs the security strategy for the ratings division, connecting corporate security objectives to business initiatives. She blends a unique mix of technical expertise and executive presence to bridge the gap that can often form between security practitioners and business leaders. Her goal is to change how we look at the security of our interconnected way of life and focus attention on defending privacy and cultivating trust.

1.2 Why all businesses should brace for impact

> **We would never expect our security guards that sit at the front of our building to defend against the military. And yet, every CISO, every security team, and every small business across America is expected to be able to protect their organization against military-level attacks.**
>
> **– Sandy Dunn**
> CIO/CSO, BreachQuest

Geopolitical tensions have escalated during a moment when the cybercrime threat level is already high.

If 2021 was the "year of ransomware," the prognosis for 2022 is no better. The frequency of ransomware events hasn't slowed in recent months even as some companies, such as those affected by the Kronos software outage, continue to cope with the wreckage from last year's attacks.

At the same time, most organizations find themselves more vulnerable than ever due to still-significant numbers of remote workers. That means increases in remote access, the rise in use of potentially unsecured networks, and – most IT professionals assume – generally less cybersecure behavior in a work-from-home environment.

Under these conditions, traditional cyber hacking techniques thrive, opening the door to malware, breaches, and a slew of other malicious cyber threats.

Phishing attempts, for example, have been either more frequent or more successful recently, since their presence in breach events has increased eleven percentage points since 2020 — up to 36% last year.

For state-sponsored cybercrime, these vulnerabilities present opportunities. That's why experts suggest it's not only government organizations, banks, and companies supporting critical infrastructure that need to be on guard from cyberwarfare.

If not by a direct hit, such as a DDoS attack, there are a number of other ways for businesses to suffer from the impact of collateral damage or be compromised as part of a more global attack.

Finally, even cyber insurance is not a silver bullet and certainly no replacement for excellent cyber hygiene and secure protocols. Following the Merck ruling from earlier this year, it's possible that war exclusions will include cyber events in the future — threatening reimbursement and assistance for acts that fall under the umbrella of state sponsorship.

Despite the risk, many businesses remain woefully unprepared and are likely to now look to their technology leaders for guidance.

2 How to get the resources you need from leadership

Here's the experts' top tips for winning support from members of the leadership team or board of directors — to help you take cybersecurity from the backburner to center stage.

2.1 Use the news

> My message around the whole topic of this cyberwarfare is to use it to educate everyone on pushing forward good security practices within their organization, the stuff that we've all been just begging everyone to do for ... 20 years.
>
> **– Sandy Dunn**
> CIO/CSO, BreachQuest

While post-breach is a good (and necessary) time to talk about cybersecurity, why wait? When major cyber events make the news, that's an opportunity to reflect on whether your business could withstand a similar situation.

This might be especially helpful to get support for some of the less sensational but equally important security measures that pertain to product lifecycle management and vendor validation, for example.

Per Miller, “all of those components that are so hard to win support for, we've got an opportunity right now to show how they bring business value, and that is so crucial when you can sit down and say ‘here's how we're going to make this better.’”

Making the connection to a real-world situation will help connect the dots and speak to the “why.” So prepare to draw from recent examples or have stats handy for support.

2.2 Play the long game

At the same time, there’s no need to wait for a significant event or crisis to discuss the needs of your team.

Per Gibson, you should share your cybersecurity wish list between budgetary conversations too, since “a lot of times you balance needs versus lack of resources.” If “you're constantly evangelizing [cybersecurity]” and the CEO begins to understand your needs, then “when resources become available they start coming your way.”

2.3 Speak their language

Getting buy-in from the CEO is part of the job, according to Gibson, but the thing is “that [they’re] going to be more interested in protecting the revenue stream and brand reputation, so those are the points that you work up to [them].”

That’s why, to give your initiatives the best chance at being taken up, you should draw a parallel between enhancing cybersecurity and achieving the organization’s goals.

2.4 Prioritize and be concise

It's important to find a balance in your message. While the current landscape presents an urgent threat, don't "run around like chicken little," per Miller.

> **I mean, the sky is not falling per se, but what's happening right now is we're getting a lot of information from a lot of different sources about these different vulnerabilities that they're exploiting ... so I think the good security teams right now are realizing we have to take this information – we really got to actually understand it in the context of our business a little better and decide what are the right steps for us to take and prioritize that...**
>
> **– Alyssa Miller**
> BISO, S&P Global Ratings

Dunn agrees that, in the face of an evolving threat landscape, it's important to "untangle the noise" for your team.

2.5 Get incident response signoff (in advance)

According to Gibson, "it's not if you get attacked: you're going to get attacked, you're going to get hit." That's why, Dunn added, that it's essential to "take a backwards approach [and] look at your incident response" and, in Miller's words, to "build resiliency and not just defenses."

This pertains to conversations with the leadership team in two important ways. First, in setting the expectation that a breach or impact from a cyber event is at least highly likely. Second, taking the opportunity to have a productive conversation on incident response.

During these discussions, consider getting sign off from the C-suite team regarding post-incident procedures. Though it may be uncomfortable to acknowledge the possibility of a serious cyber event, it's a conversation best had in advance, instead of under pressure.

2.6 Be transparent

> **Don’t let a good breach go to waste.**
>
> **– Alyssa Miller**
> BISO, S&P Global Ratings

In other words: use cyber incidents as a teachable moment for your team.

On the topic of building resiliency in addition to defenses, Miller identifies what “too many CISOs get wrong” about communicating incidents. Breaches and other cyber incidents are an opportunity for cybersecurity advocacy.

Instead of pointing the finger at the vulnerabilities that allowed for the incident to occur, focus on the positive. Say, “Here's the things that we did as part of our program that limited [the impact]. Here's the next logical steps we need to take that we haven't done yet where I'm going to need additional funding to expand on our capability to address what we don't have coverage for today.”

Doing so will validate your existing cybersecurity initiatives, establishing your credibility as the security leader, according to Miller.

3 How to get buy-in from your teammates

Support from leadership is great, but all the proper protocols and cybersecurity software in the world won't matter if they're not being deployed properly by your team. Here are some tips from experts that will help you communicate cybersecurity initiatives to your team more effectively.

3.1 Make it relevant

> **Education, education, education.**
>
> **– Sandy Dunn**
> CIO/CSO, BreachQuest

It's likely that as far as initiatives go, education is already at the top of your list. On what type of actions should be taken to protect businesses, all experts agreed that education should be top priority.

But in addition to the baseline, Miller suggests "getting away from the traditional 'just awareness' training and finding other ways" to educate your team. Including, Miller suggests, having more transparent communication regarding past cyber incidents or close calls.

Speaking in more detail about how cybersecurity protocols have succeeded (or failed) in the past will help stress the importance of adhering to them by communicating that the threat is real.

And a more tailored approach to education is likely to garner more interest: one that is relevant to each team's most important vulnerabilities. For example, since one in five spear-phishing emails target employees in sales roles, according to a 2021 study by Barracuda, those teams should receive beyond the standard spiel on how to detect a threat by email.

Consider layering education by access: It's important not to assume that senior staff members or anyone with access to sensitive data "knows better." Our research suggests that, at least as far as passwords are concerned, despite being higher risk for targeted attacks members of management and C-suite use weak ones just as often.

Per Dunn, "the most dangerous person is inside your network, but also the person that can help you the most is inside your network," underscoring the importance of empowering your team with relevant training.

3.2 Make it easy

According to Dunn, it's critical to "get away from manual anything that requires manual intervention — it's gotta focus on automation."

Miller adds that when implementing cybersecurity protocols, it's important that "our engineers feel empowered and enabled with the right tooling and processes... without slowing down the business..."

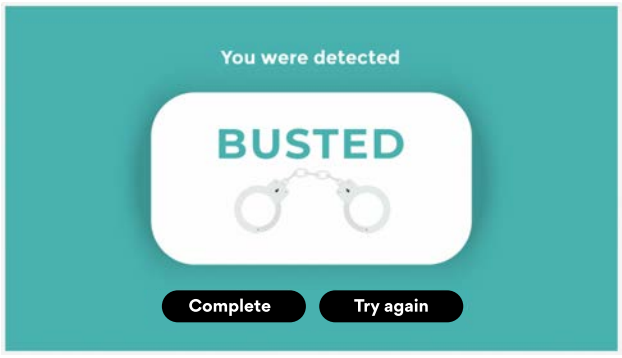
In other words, "making it easy" is likely to involve empowering your team with software that serves business efficiency as much as cybersecurity.

A prime example is a password manager, which speeds up on-and-off boarding and facilitates credential sharing while making strong passwords and multifactor authentication possible.

3.3 Make it fun

Even while education is relevant and cybersecurity software means it's baked into processes, some aspects of cyber secure behavior can (still) feel like taking medicine. The antidote? Make it fun.

In the short run, consider gamifying education and training.



Nord Security's Security & Risk Awareness Training 101 course: from the Physical Security chapter on "piggybacking."

For the long term, test your team: through tabletop exercises and internal-facing phishing expeditions, for example.

These immersive activities promise to make secure behavior a point of pride and achieve buy-in "by encouraging the best you can your entire organization to be active in the defense too and rewarding them..." says Gibson.

3.4 Be supportive

You can't underestimate the importance, according to Gibson, of providing your team with support. When responding to questions around things like suspicious emails, Gibson tells his team, "just send it to us, I got your back" — suggesting that encouraging open communication will pay off in the long run.

Gibson continues, "you want to build that old culture where people can say 'I think we got an issue here.' Then you go, 'Yeah, all right. I'll go chase it to the ground and you've got my full support,' versus a zero tolerance of defects-type issues and they're afraid to do that..."

Remember that your attitude and approach will have an impact: A positive take and open ear may keep you from being kept in the dark when it matters.

4 Conclusion

4.1 Summary

Nothing is certain but death, taxes, and cyber threats. But while the more cyber aware among us have been banging the drum for cyber threats since the dawn of the internet, the current threat climate is indeed something new.

As the cybercrime industry is booming and businesses are suffering from more frequent and more financially devastating cyber events, it can be difficult to communicate the threat level without coming across as alarmist. And when causes compete for resources, your internal communication strategy is just as important as your security savvy.

When advocating for measures to leadership, it's important to stay current, be consistent, and prioritize. When it comes to your colleagues: accessibility and ease are key.

5 Next steps: Start building your defense with NordPass Business

5.1 NordPass Business: an easy win to bolster your defense strategy

Businesses can be disrupted by cyber warfare in many ways — whether as a direct target or collateral damage. And while the motivations of state-sponsored actors differ, they have one habit in common with run-of-the-mill cybercriminals: they start with the lowest-hanging fruit.

In many cases, that means exploiting the vulnerability of weak, reused passwords, which, despite awareness of their danger, remain surprisingly common across industries and roles. In fact, depending on the type of attack, up to 80% of successful breaches may be caused by the use of stolen credentials, according to Verizon's 2022 Data Breach Investigations Report.

With NordPass, you can all but eliminate poor password hygiene vulnerability while increasing your team's efficiency — something both your leadership team and colleagues will love.

5.2 Why your leadership team will love NordPass Business

Most password managers offer the same promise: to enhance cybersecurity by storing, organizing, and autofilling complex, hard-to-crack passwords. But NordPass Business adds additional cybersecurity features to your arsenal, including:

- ✓ A Data Breach Scanner that scans the web for breached domains, credit cards, and personal information (in addition to passwords).
- ✓ Company-wide password health metrics.
- ✓ A detailed Activity Log.

NordPass has the most encrypted document storage, the highest level of authentication security (2-step), and is the only password manager using fast and secure XChaCha20 encryption.

5.3 Why your teammates will love NordPass Business

NordPass prioritizes user friendliness — and it shows. NordPass Business clients have described the app as “easy to use and extremely handy” and said it “saves [them] hours during the workday.” What’s more, 24/7 support means you are never never left in the lurch.

Contact us

Ieva Labutyte, NordPass:
ieva.labutyte@nordsecbusiness.com
+370 674 75363

Simas Zvirblis, NordPass:
simas.zvirblis@nordsecbusiness.com
+370 681 27735