XM Cyber

A CISO's Guide to Reporting Cyber Risk to the Board

XM Cyber

Table Of Contents:

Reporting Cyber Risk: Even When It's Done, It's Rarely Done Right 4

The Challenges of Reporting 5

How Current CISO Reporting Fails to Meet These Challenges 6

A Better Way to Report Risk 7

How XM Cyber Protects Critical Assets and Crystallizes Causality 8

Six Key Security Questions XM Cyber Answers 13

Healing the CISO/Board Disconnect 14

XM Cyber

Just how elevated have the cybersecurity stakes become for today's organizations?

Consider this: In the wake of the recent high-profile ransomware attack on Colonial Pipeline, the United States Justice Department announced it would give cyber-attacks and conventional terrorism the same investigative priority.

In other words, government officials perceive the potential risks of cyberattacks to be on par with the most heinous acts of terrorism.

Yet while protection from ransomware attacks and other cyber-threats is clearly a strategic objective for today's organizations, that goal is jeopardized by a persistent problem: There is a disconnect between your position (CISO) and the board to which you report – a failure of communication that leads to misunderstanding, unnecessary risk and "worst-case scenario" cyberattack outcomes.

Let's take a closer look at why this disconnect exists and explore a better way to help you articulate cyber risk to your board.

XM Cyber

Reporting Cyber Risk: Even When It's Done, It's Rarely Done Right

In terms of understanding risk, you sit in a privileged position as a CISO. Yet many organizations are failing to reap the benefits of regularly plugging into your perspective.

A 2021 Ponemon Institute study showed **only 7%** of CISOs report directly to their CEOs. Meanwhile, **roughly 60%** of CISOs "regularly brief" their board of directors.

Even worse: Among that **60%**, nearly half report such briefings occur exclusively in the wake of a newly discovered security problem.

Those aren't the only concerning numbers.

The majority of cybersecurity leaders report being at least three steps away from the CEO in the reporting structure, while **only 37%** report that their organization effectively leverages their expertise.

According to Gartner, **ONLY 10%** of boards have a dedicated cybersecurity committee overseen by a board member, though that number is expected to quadruple in just 5 years.

Encouragingly, however, the percentage of board-level leaders who view cyber security as a direct business risk has risen from 58% to 88% between 2016 and the beginning of 2022.

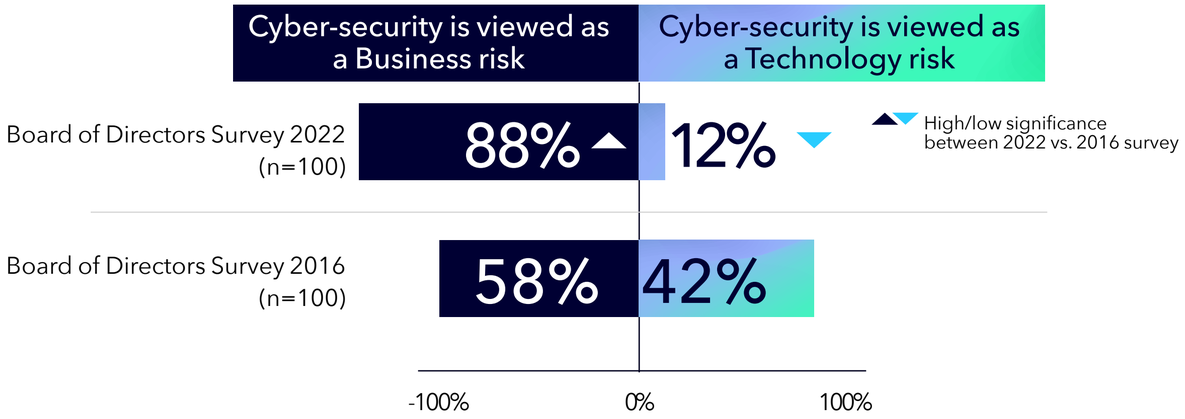


Fig. 1: 2022 Gartner View from the Board of Directors' Survey

These numbers make it clear that serious shortcomings exist within corporate reporting structures and board reporting procedures. Yet even as your involvement as a CISO becomes more direct, the problem of effectively communicating risk to the business remains.

XM Cyber

The Challenges of Reporting

When reporting risk as a CISO, you must wrestle with the question of explaining technical problems to a largely non-technical audience.

When one is extremely well-versed in a subject, it's not always easy to know where to begin when conveying information to people with less grounding. The "curse of knowledge" often rears its head in board reporting scenarios, so it's important to make sure that problems, solutions, value propositions etc. are all clearly and concisely articulated in business language.

It also helps to have clear and quantifiable metrics to lean on. These metrics will ultimately impact key decisions on budget, resources, and affect the overall security posture of the organization.

4 Key challenges organizations face when reporting risk to the board

The ability to quantify the risk of breach to business-critical assets across on-premises and cloud environments through a single pane of glass.

Identifying the risk of potential M&As and the steps necessary to mitigate them.

The path of least cost for maximum impact on the organization's security posture and where to focus remediation efforts to get there.

The impact of security investments to security posture over time.

Historically, IT was once perceived as a massive cost center with limited impact on the bottom line. Cybersecurity still sometimes falls under that shadow today.

Shifting the perception of cybersecurity from cost center to business enabler should be a key priority for CISOs. That's not always easy to do without a simple and intuitive demonstration of ROI on security investments. Part of this includes quantifying risk in a way that truly reflects what is at stake.

XM Cyber

How Current CISO Reporting Fails to Meet These Challenges

A common, flawed approach to reporting is the recitation of conventional figures (how many vulnerabilities, incidents, patches etc. and how those numbers change over time) without applying real insight. This approach is a rough yardstick of progress. Lengthy discourses about security team actions, based on conventional metrics, can create white noise and obfuscate the real heart of the matter:

Are Our Most Important Assets Safe?

Probability Is Another Area Where Wires Are Crossed.

Probability can be calculated in different ways. First, we can examine statistical data. It's possible to extrapolate probability from analysis of past statistical data, but this omits the context of a specific organization – the threat landscape, changes in the environment etc.

Ultimately, CISOs need to convey the full picture of risk. For example, security risks correlated with business criticality, security posture, risk registers, and change management systems.

Without a refined understanding of critical asset risk, it's impossible to answer questions such as "Are we secure?" or "Are we improving?"

And without real answers to those questions, risk reporting becomes an academic exercise.

Risk can be simply explained as the intersection of probability and impact:
How likely is a successful cyberattack and what would be the cost to the organization if this occurs?

XM Cyber

A Better Way to Report Risk

To understand whether an organization's most critical assets are safe, it's imperative to have visibility into how things change over time, and how those changes affect risk.

Modeling to predict the likelihood of an attack is one way to do this. This approach provides a consistent predictive model that cuts through the noise of what can be bypassed, and what cannot, and contextualizes this information within the framework of critical assets.

Boards need to understand the likelihood of compromise and the impact that could occur to business-critical assets. These risks should be contextualized to each part of the business. For example, risks to ERP services, business services, cloud environments, customer databases etc.

Most importantly, they need answers to the key questions:

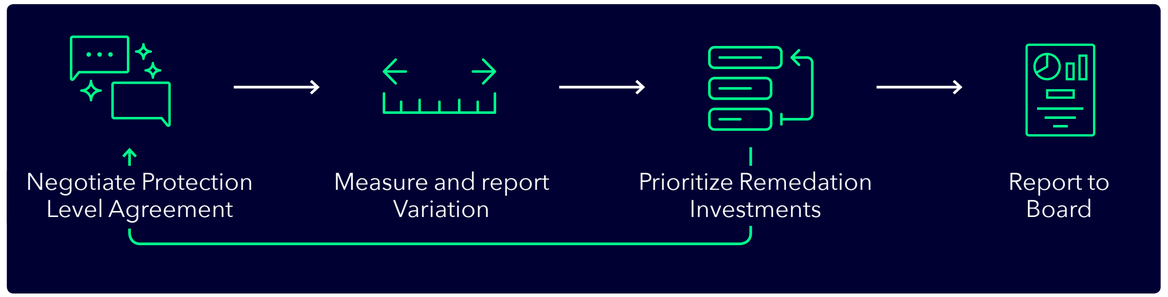
- What can be compromised today?
- What is the likelihood of that happening?
- What is the aggregate impact?
- What is the level of operational risk?

Boards need visibility into business insights and real-world ramifications. They need to understand the efforts being made to reduce risk and how these efforts are paying off.

In the face of an incident, will your stakeholders stand up in front of the cameras and defend their cyber security investments?

As a CISO you must explain the business value of any security investment you make and have metrics that define specific, agreed-upon protection levels.

More importantly, when reporting risk, it is not about security tools but the actual metrics that drive business decisions. Nonetheless, a CISO must be able to defend their security program with their key stakeholders. If your reporting delivers on outcomes and not a laundry list of issues, you can realize your organization's goals.



Fortunately, XM Cyber has created technology that makes conveying the answers to those questions to a non-technical audience as simple as possible.

XM Cyber

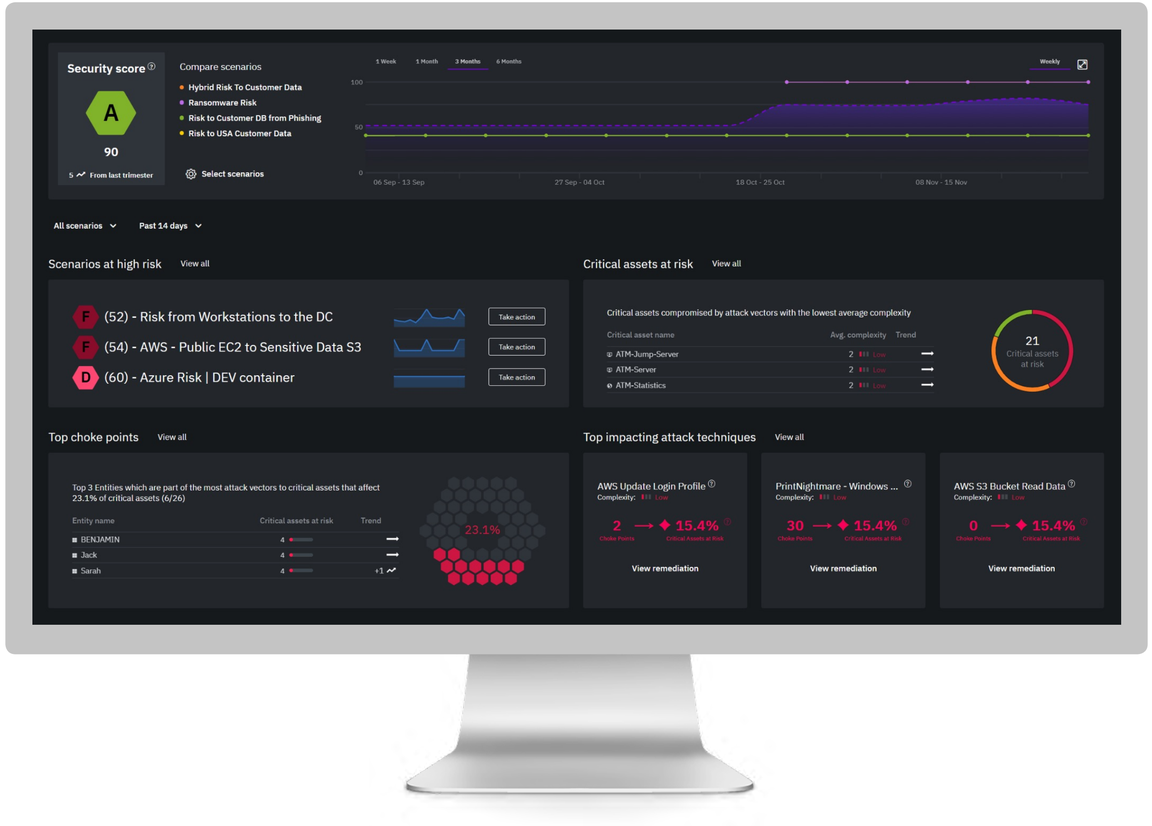
How XM Cyber Protects Critical Assets and Crystallizes Causality

XM Cyber helps organizations understand how attackers can compromise their critical assets across any environment - on premises or in the cloud.

Our technology uses sophisticated attack modeling to map all possible attack paths an attacker could take due to misconfigurations, vulnerabilities, overly permissive identities etc. to compromise business-critical assets. XM Cyber then quantifies the risk to your critical assets and shows which techniques can be used to get to them, focusing remediation efforts.

By providing a graphical visualization of an organization's attack surface, XM Cyber makes it possible to see through the eyes of an adversary. Our technology makes it simple to see precisely how a combination of exploits chain together to form attack paths from breach points to critical assets.

XM Cyber's Attack Path Management platform provides a dashboard that enables you to monitor your environment's security posture at a glance. It provides you with actionable intelligence so you can tackle your scenarios, secure your critical assets, fix the choke points, and remediate the attack techniques.



Unified view to track all critical assets providing continuous cyber security posture management via the XM Cyber APM platform

Security Score -

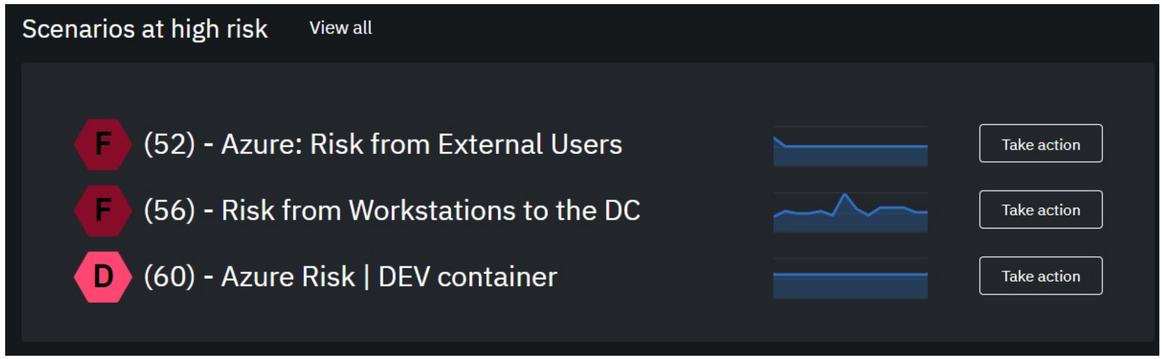
The security score widget shows the average security score of all the scenarios running in your environment. Once attack scenarios have been sufficiently modeled, XM Cyber scores the level of risk to the organization. The score of a scenario is based on how easy it would be for the attacker to compromise the critical assets. As you remediate security exposures, the security score improves, indicating better IT hygiene.

Compare Scenarios - Below the score, you can see whether you're trending up or down in the time range selected.

When you use the Compare Scenarios trend graph you gain immediate insights into:

- Whether your scores are trending up or down because of network changes, M&A activity, new third parties connecting to your environment etc. and what critical assets are at risk.
- How quickly you respond to sudden drops in a score.
- How current or new security investments are contributing to your overall risk level.
- How to identify processes that run periodically and impact the level of security.

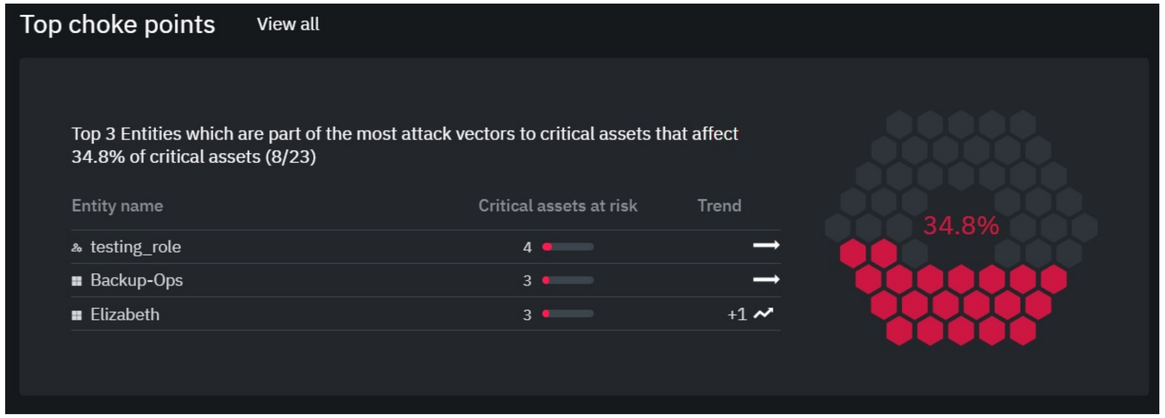
Scenarios At High Risk – XM Cyber enables you to prioritize which scenarios to improve first. When you view all the scenarios at high risk, you view the scenarios with the lowest scores and improve these scenarios first. You can even view a specific scenario and its trend by drilling down or you can "take action" to tackle this scenario and follow prioritized guided remediation steps.



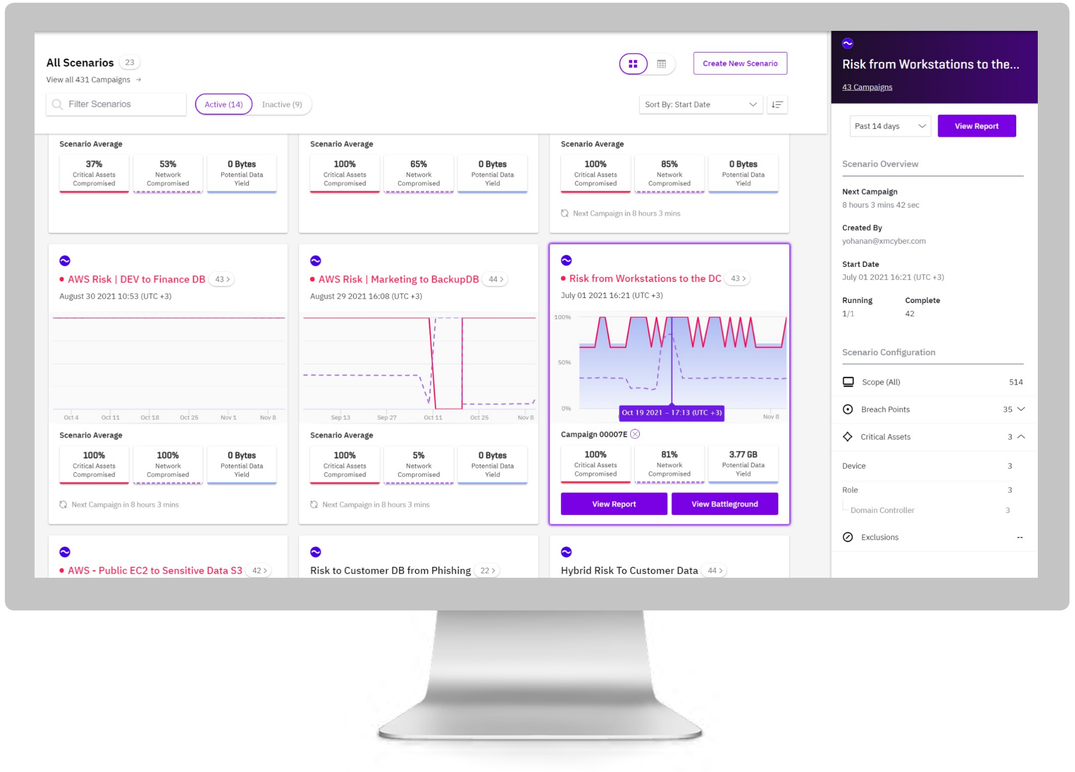
Critical Assets At Risk – You can also prioritize which critical assets to secure. The table shows the critical assets that are at risk and the attack paths with the lowest complexity. Paths with low complexity are easier for the attacker to compromise. The ring graph breaks down your critical assets by the complexity of the attack paths leading to them. A sizable percentage of your critical assets are on attack paths with low complexity, so harden these critical assets first.

XM Cyber

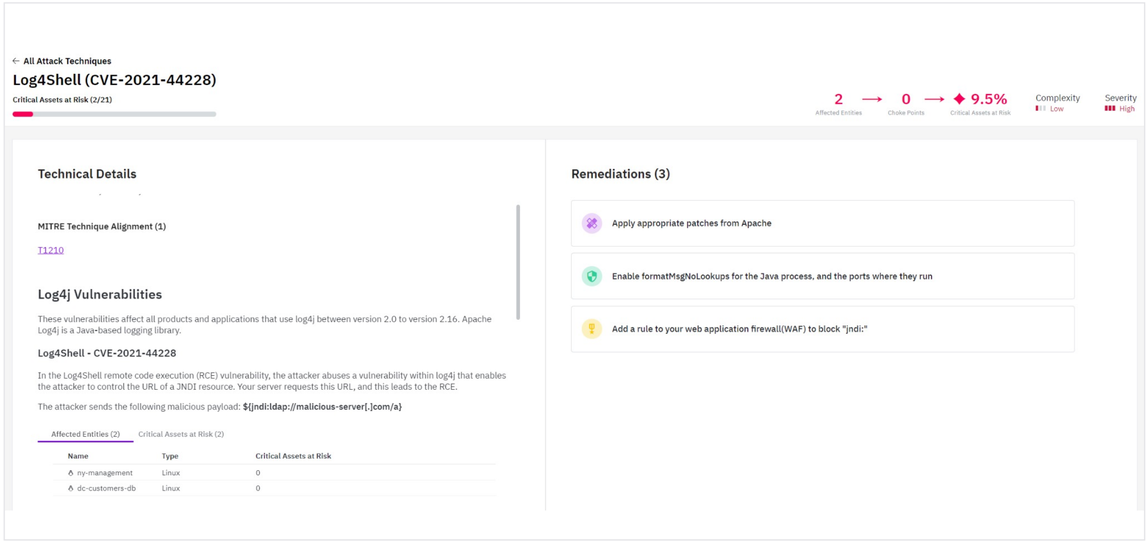
Top Choke Points – The table shows the three entities that attack paths most frequently cross on their way to your critical assets. These are the choke points in your environment. They put your critical assets at the most risk. The graph shows you the percentage of critical assets that the top three choke points lead to. Fix these top three choke points first. It won't necessarily harden all your critical assets, but it will give you high ROI of least cost and maximum impact to your security posture. Drill down into the choke point to disrupt the most damaging attack paths and follow prioritized guided remediation steps.



Prioritized remediation helps ensure that security teams fix the most pressing issues, while security scores update in real time to show the likelihood of compromise. Risk can be broken down by specific scenarios. For example, XM Cyber can show whether an attacker can move from marketing endpoints to a customer database.



Attack modeling scenarios aligned with business goals to focus security posture hardening



Automated reporting and guided remediation steps based on the path of least cost for maximum impact

In essence, XM Cyber allows boards to quickly grasp:

- How their organization can be attacked.
- How improvements are occurring over time because of security investment, change in processes or implementation of environment hardening.
- How much risk exists for critical assets.

XM Cyber

Six Key Security Questions XM Cyber Answers:

1
What percentage of my critical assets are at risk at any given time?

2
What are the risks?

3
What do we need to remediate first to significantly impact our risk level?

4
Are our investments paying off? Are my protection levels increasing?

5
Do we have sufficient resources to handle the risks?

6
How are we improving over time?

Cost-effective prioritized remediation reduces attack surface and hardens security posture

XM Cyber

Healing the CISO/Board Disconnect

CISOs have historically struggled to connect with boards and convey a clear picture of risk in relation to the business and what return on investment their security stack is delivering.

Fortunately, XM Cyber provides the tools you need to bridge that gap and deliver a straightforward and quantifiable presentation of risk and ROI.

Ultimately, you need more than the right message – you also need the right tools. By centering critical asset risk – and providing the technological framework to contextualize and mitigate that risk – XM Cyber helps ensure that board members walk away with a much more powerful understanding of the most essential question they will likely ever face:

Are Our Most Important Assets Safe?

Visit XM Cyber to learn more: www.xmcyber.com

https://www.gartner.com/en/newsroom/press-releases/2021-01-28-gartner-predicts-40--of-boards-will-have-a-dedicated-

https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/

https://www.forbes.com/sites/forbestechcouncil/2021/09/08/why-your-ciso-should-report-directly-to-the-ceo/?sh=51c346f33533

Gartner Report: Treat Cybersecurity as a Business Decision, Paul Proctor, 2021

Gartner, Five Steps to the Best Security Metrics Ever, Jeffrey Wheatman, 2021

About XM Cyber

XM Cyber is a leading hybrid cloud security company that's changing the way innovative organizations approach cyber risk. Our attack path management platform continuously uncovers hidden attack paths to your critical assets across cloud and on-prem environments, so you can cut them off at key junctures and eradicate risk with a fraction of the effort. This approach is a complete game-changer, which is why some of the world's largest, most complex organizations choose XM Cyber to help eradicate risk. Founded by top executives from the Israeli cyber intelligence community, XM Cyber has offices in North America, Europe, and Israel.

xmcyber.com

XM Cyber

Tel-Aviv: +972-3-978-6668
New-York: +1-866-598-6170
London: +44-203-322-3031
Munich: +49-163-6288041
Paris: +33-1-70-61-32-76