BinaryCore

15 November 2022

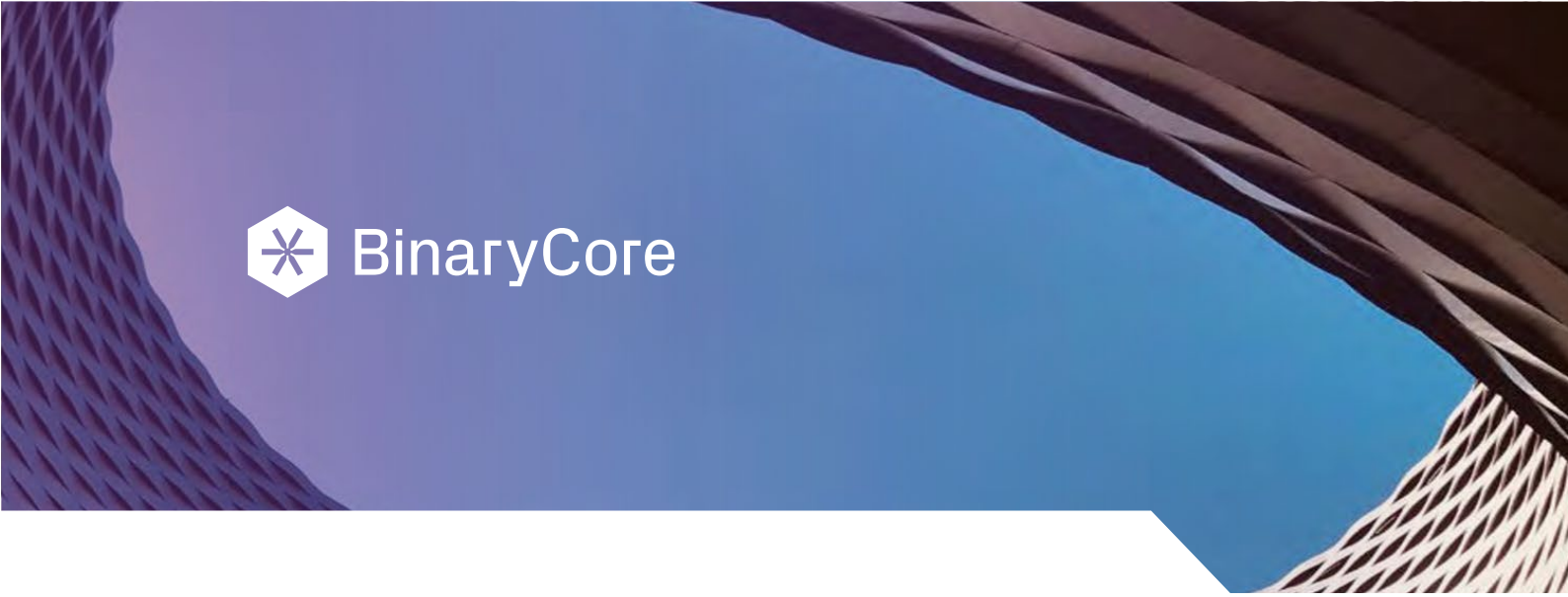
CEO proactiveness: a winning cyber response strategy

Authors:

Guy Ngambeket, Michael Roemer, Ronny Schubhart and Clif Triplett

For businesses of all sizes, and across different industries, the threat posed by cybersecurity attacks is increasing dramatically. There is already a $1 trillion cost in the US and Europe alone related to cybersecurity disruption to supply chains, and that cost is only becoming steeper.

A rise in geopolitical tensions—sparked by the conflict in Ukraine and continuing animosity between the US and China—has led to a proliferation of cybersecurity attacks in 2022. As a result, there has been a 360 percent year-on-year increase in



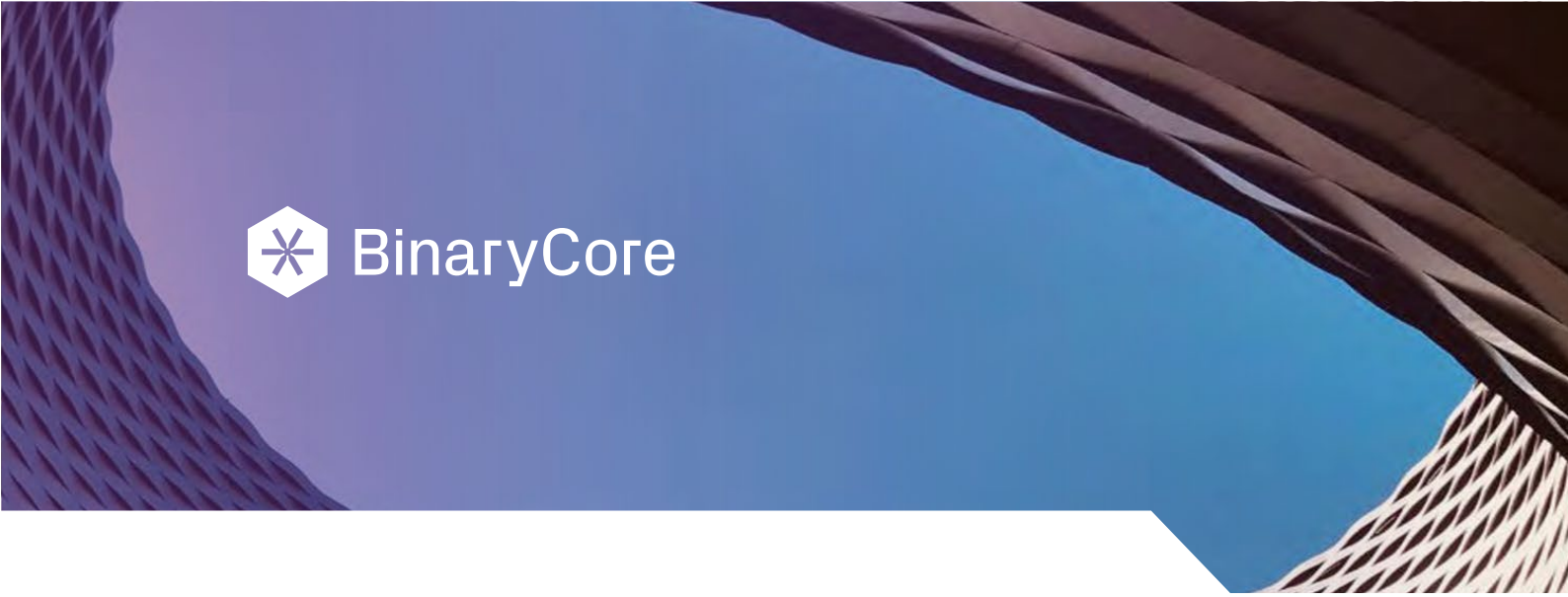
the damage inflicted by cybercrimes this year compared to 2021, while it is predicted that more than 33 billion records will be stolen by criminals by the end of next year. By 2025, cybercrime could inflict up to $10.5 trillion in damages.

By 2025, cybercrime could inflict up to $10.5tr. in damages.

It's not just multinational companies, or those in industries that are of national strategic interest, that are targets. In fact, the contrary is often true. A study in Germany showed that 84 percent of companies have experienced more attacks than ever before at an alarming rate, with small and medium-sized businesses being the main targets—collectively costing the companies involved around €203 billion.

After all, cyberattacks can and do affect any company that is connected to the Internet. Little surprise, then, that the Allianz Risk Barometer 2022 placed cyber incidents as the number one concern for risk management experts worldwide. More than half of network engineers and chief information officers (CIOs) also agree that cyberattacks are among the biggest risks their organizations are currently confronted with.

High costs

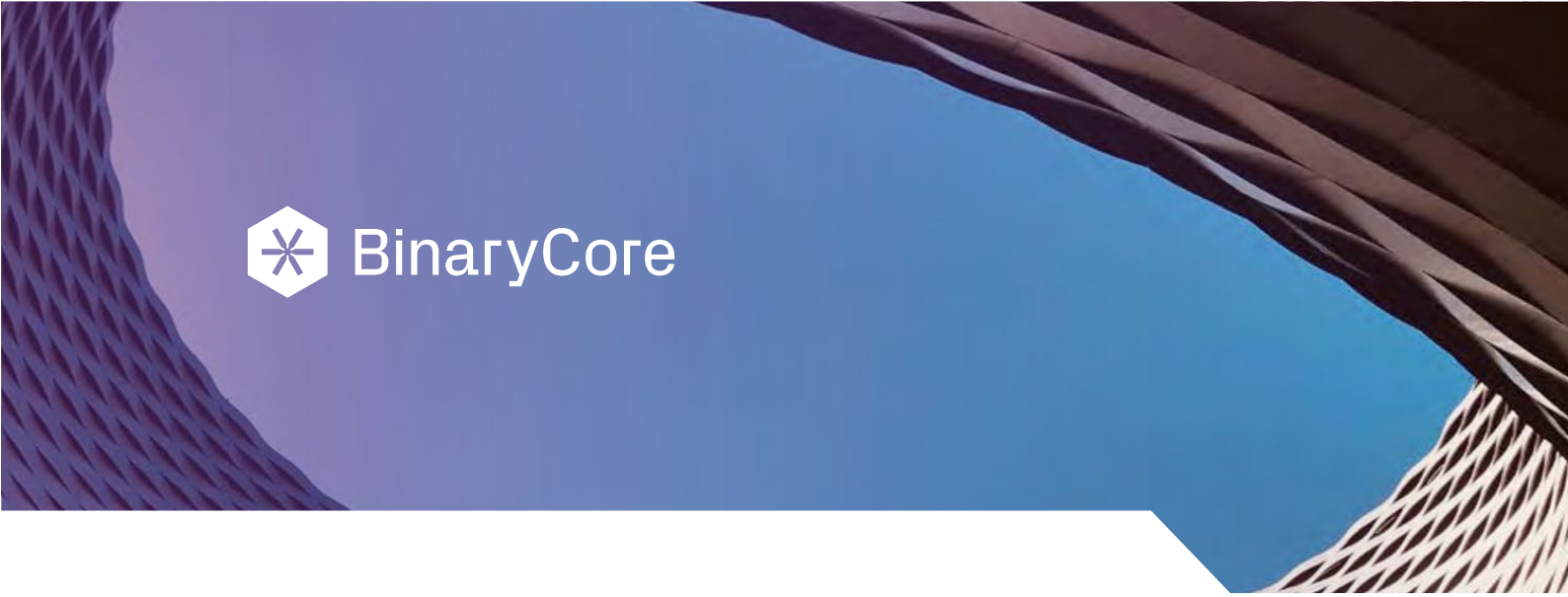


This recognition of the risk of cyberattacks is because the consequences of such events can be devastating—both reputationally and financially (see figure). Many firms have even gone bankrupt as a result of security breaches. In 2014, code hosting company Code Space suffered a major distributed denial-of-service (DDoS) attack, which caused huge disruption to their clients. The very large sums required to recover their databases and regain control meant the firm became inoperable. British telemarketing firm The Heritage Company also had to shut down in 2019, after more than six decades in business, after suffering huge losses from a ransomware attack.

Figure
The consequences of cyberattacks can be devastating

Industry	Top cyberattack types	Main purpose	Main damage types
Manufacturing	**Denial of service**	Disturb or stop business activity	— Stopping of sales — Supply chain distortion — Production slow down
	Account takeover	Data exfiltration	— Loss of intellectual property — DSGVO fine — Damaged brand
Banking/finance	**Phishing**	Data exfiltration	— DSGVO fine — Loss of intellectual property — Damaged brand reputation
	Web application attacks	Data exfiltration	— Loss of intellectual property — DSGVO fine — Damaged brand
Vital infrastructure	**Ransomware**	Financial theft	— Loss of funds — Production ceasing for several days or weeks — Image loss

Source: Kearney analysis

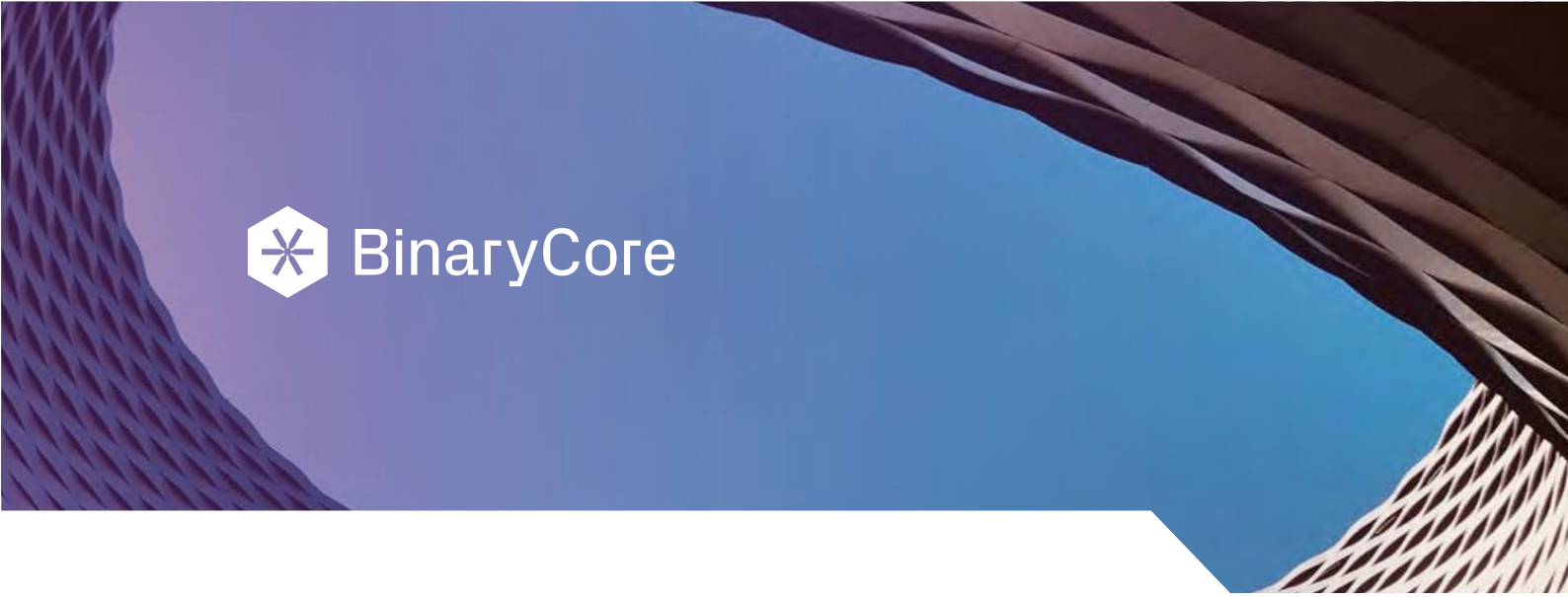


Because of the potentially enormous consequences of a cyberattack, more businesses are dedicating significant amounts of capital to cybersecurity. Even as the global economy moves into more difficult times, the amount of money dedicated to securing businesses from a breach continues to increase. Indeed, cybersecurity spending globally is expected to surpass $200 billion by 2024. While investment over the past decade has been largely targeted at companies' IT systems, investment is now shifting to the new generation of cloud systems. Although greater investment in cybersecurity solutions is welcome, this focus on the cloud has meant that the security of operational technologies (OTs) has been underserved. This is potentially leaving gaps in the defenses of vital infrastructure for criminals to exploit.

Cybercrime industrialization

One of the challenges companies face when attempting to monitor cybercrime is that the practice has become increasingly professional.

The criminal industry has become more organized, with illicit groups finding access points to companies and then selling this information to other criminals on the market. Partly this is because cybersecurity is a relatively "safe" crime to commit—only 0.3 percent of reported cybercrime complaints are enforced and prosecuted.

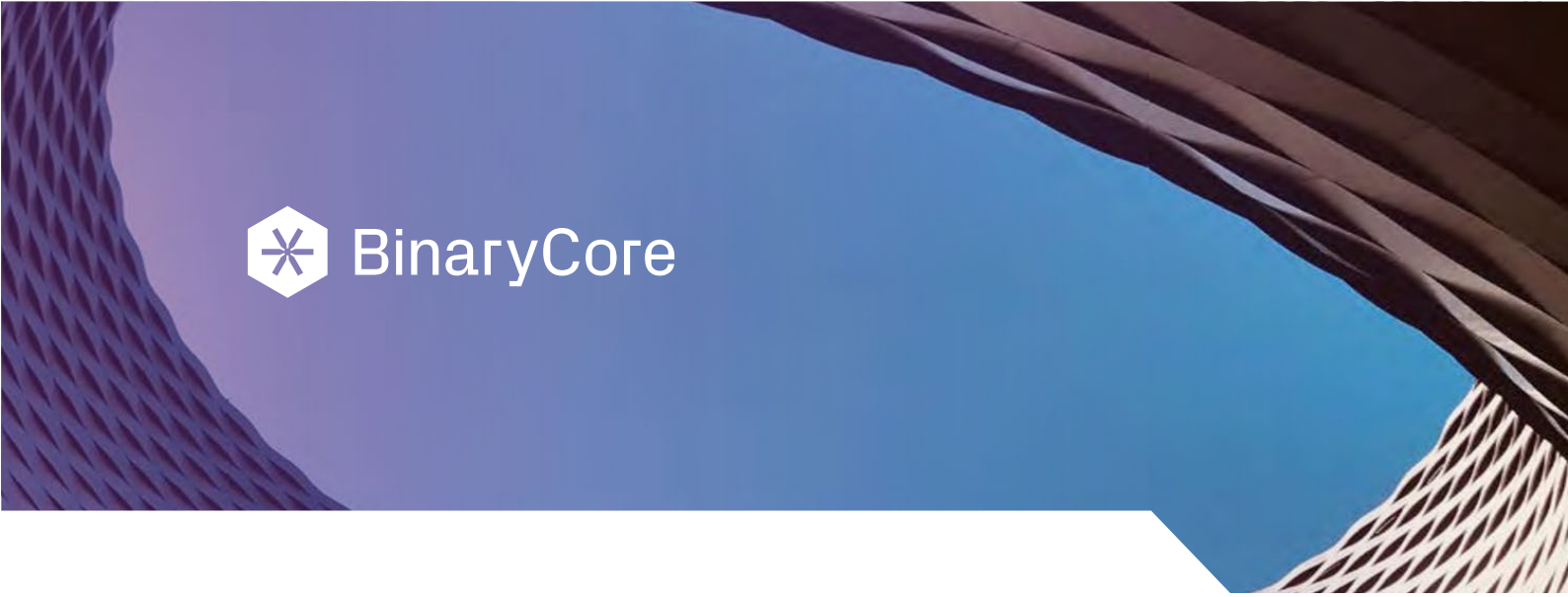


Only 0.3 percent of reported cybercrime complaints are enforced and prosecuted.

This has fed into an "industrialization" of the space—which in turn has caused entry costs to come down. Criminal groups can now purchase packages that allow them access to companies' systems, such as through DDoS or ransomware attacks. Third parties are also providing "ransomware-as-a-service" packages to allow criminals access to business networks.

A fifth (20 percent) of all attacks are now executed via trojans, which are sold as commodities for relatively small sums. Just $40 worth of investment in such packages a month is enough to commit attacks that can return up to $25,000. The risks posed by cybercrime are increasing by the day—making it more essential than ever that companies take proactive steps to patch any deficiencies and strengthen their resilience.

Just $40 worth of investment in such packages a month is enough to commit attacks that can return up to $25,000.



Common weaknesses

What are the main vulnerabilities that allow criminal groups to gain access to businesses' crucial data?

There are various identifiable triggers which suggest that a company may be at higher risk of cyberattacks. Exposed usernames and weak passwords can give bad actors an easy way in. A lack of operational technology (OT) security, or minimal incident detection capabilities, frequently means that attacks aren't detected for a long period of time. Indeed, 287 days is the average amount of time advanced persistent threats (ATPs) stay within a system before being identified and dealt with.

A lack of investment in this kind of technology also makes companies more vulnerable to phishing exploits—particularly when access controls are also weak or the local IT environment has been compromised.

However, one of the most common sources of risk comes from third parties. A common mistake is known as "assumed trust." Companies simply presume that their suppliers must have resilient cybersecurity procedures in place. But in practice, around 50 percent of attacks that companies suffer are because one of their suppliers or partners down the supply chain has had a vulnerability exploited. It's no longer enough for businesses just to consider their own capacities to resist

cyberattacks. Rather, all firms should be taking strong measures to build resilience down the supply chain—and ensure all their partners are benefiting from equally sophisticated protection.

Prioritization of actions

How do leaders go about establishing the right strategy—the one that will put them in the ideal position to detect and respond to cyberattacks?

Doing so is a challenge because every company is dealing with limited resources. In an ideal world, everybody would invest vast sums to ensure near-total protection on every single asset. In practice, of course, this isn't possible, particularly as we enter more difficult economic times.

When considering what a cybersecurity strategy should look like, the first step is to prioritize. Executives must ask themselves which of their assets are the most vital. Which ones are at the greatest risk and, if compromised, would cause the most damage? These assets should be prioritized for investment and protected first. By focusing cyber-protection on vital assets, firms will also achieve the "shadow effect" of protecting many other assets within the organization as a result.

The next step is for executives to think about what an acceptable level of risk actually looks like in practice.

How much risk to certain assets can they tolerate? What steps will they take if circumstances change, and the risk exceeds that level? Will this trigger pre-specified risk management actions, diversion of investment resources, or both? These questions must be internalized into the decision-making process so that firms have a strong understanding of the risk landscape and the trade-offs involved. As cybersecurity threats continue to evolve, so firms should continue to ask these questions and ensure that they're assessing risk on an ongoing basis.

Proactive steps

Despite the challenges faced, and the rate at which they are increasing, it's important for senior leaders not to panic. All this will do is increase the likelihood of mistakes and, therefore, potentially give bad actors more opportunities to inflict harm.

It's also essential that companies reject "quick-fix" solutions. Many firms that are undergoing digital transformation, and shifting from on-premise to cloud solutions, believe the new technology will do the security job for them. They believe that hyperscaler servers are protected by default, and that all

entities using the server will be protected by the cloud environment. This is not the case.

Servers simply provide an infrastructure. Protecting that infrastructure from cybersecurity threats is the job of individual companies. Proactive steps are required to do this.

Cultural shifts

According to the UK's Information Commissioner's Office (ICO), human error was the cause of around 90 percent of data breaches in 2019. Employees can make a range of mistakes, such as having weak passwords, that put company systems at risk. Often this is simply because they lack the required knowledge or are not aware of how serious the consequences of their mistakes could be.

This is now true more than ever as employees increasingly work from home, potentially making the home environment an additional threat vector—and putting employees themselves at risk.

At the moment, 70 to 80 percent of cybersecurity attacks succeed because of human error, insufficient processes, organizational weakness, or blind spots. A cultural shift is therefore required in many companies to establish a security culture mindset throughout the organization. This means clear,

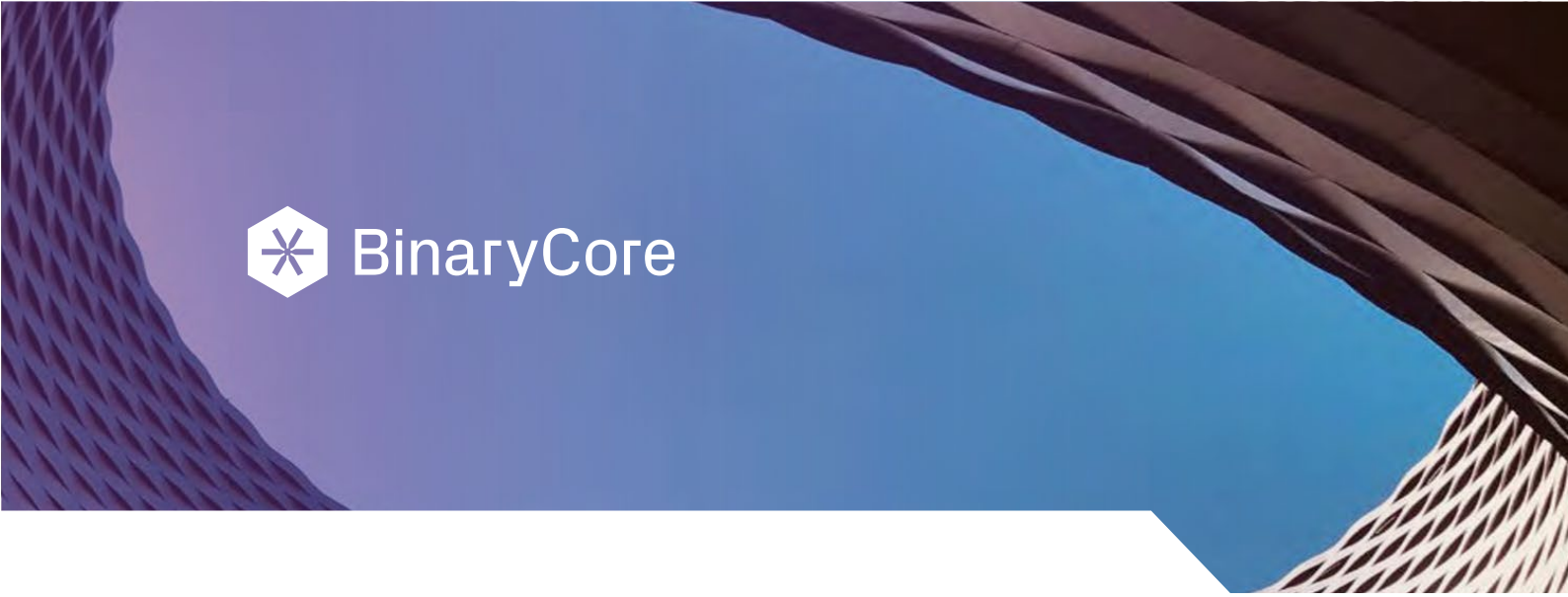
strong messaging from the very top emphasizing that cybersecurity is a high priority.

Senior, c-suite executives must communicate the importance of cybersecurity, not just for business reasons, but for the safety of individuals and the future of the company.

Seventy to 80 percent of cybersecurity attacks succeed because of human error, insufficient processes, organizational weakness, or blind spots.

While developing and articulating such a strategy must come from the top, it also requires the engagement of the entire organization. An effective cybersecurity strategy requires the technological infrastructure to put it into practice, as well as the human resources to execute the plan.

In other words, building resilience to evolving cybersecurity threats necessitates broad awareness of the risks among every individual within an organization.



Strong governance

In order for these strategies to be deployed effectively, companies also need to have strong governance procedures in place. For cybersecurity procedures to be at their most efficient, there needs to be an entire culture engrained across every segment of the organization.

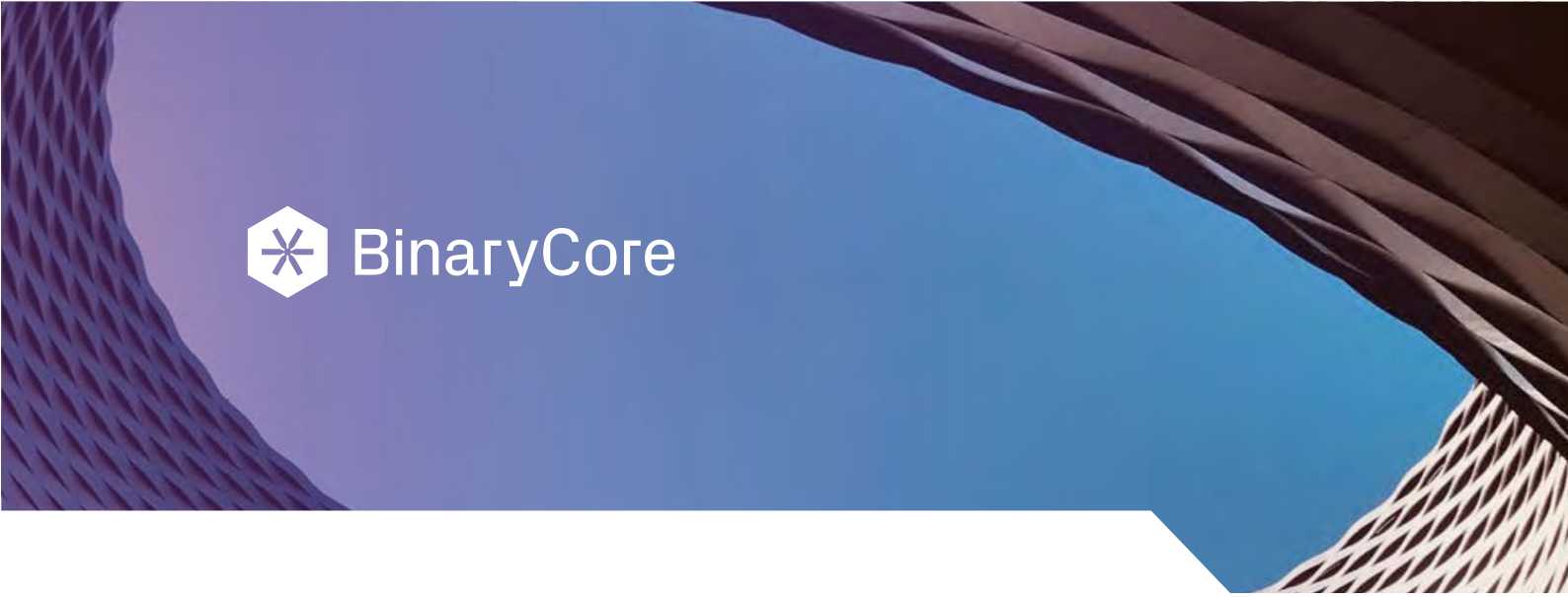
Every individual needs to be aware of their specific role and responsibilities. Senior managers and executives should provide oversight ensuring these roles are fulfilled. If and when certain functions are not being performed properly, they should also be on hand to address issues immediately filling the gaps quickly before cyber-criminals can take advantage.

Devising, implementing, and overseeing such a strategy is a tough task, but it's a crucial one for senior leaders to overcome if they wish to ensure their organizations are resilient to increasingly sophisticated cyberattacks.

Next steps

The threat posed by cyberattacks is increasing almost by the day. Attacks are growing both in volume and sophistication.

Executives must deploy resources to ensure their organization has the right frameworks in place to resist these threats successfully. That means taking proactive steps to develop a



robust strategy that deeply engrains cybersecurity concerns within a firm's business processes—and, perhaps more fundamentally, within its entire culture.

Kearney and BinaryCore, Kearney's deeptech solutions business, assist organizations with this all around the world. Our global teams work to evaluate enterprises' existing cybersecurity capabilities and highlight where improvements can be made.

By identifying vital assets, establishing companies' risk tolerance, conducting risk and impact assessments of key infrastructure, assessing supply chain cyber service level agreements, reviewing investment in cybersecurity, and evaluating existing governance procedures, BinaryCore can quantify a firm's exposure to the threats. With this information, we can help develop and implement an appropriate cybersecurity strategy that contributes to greater organizational resilience.

In so doing, we are helping leaders protect their companies' vital assets from the increasing number of bad actors who have the potential to inflict serious damage.

To read discuss any of the themes outlined in this article email us at socialmedia@binarycore.com.