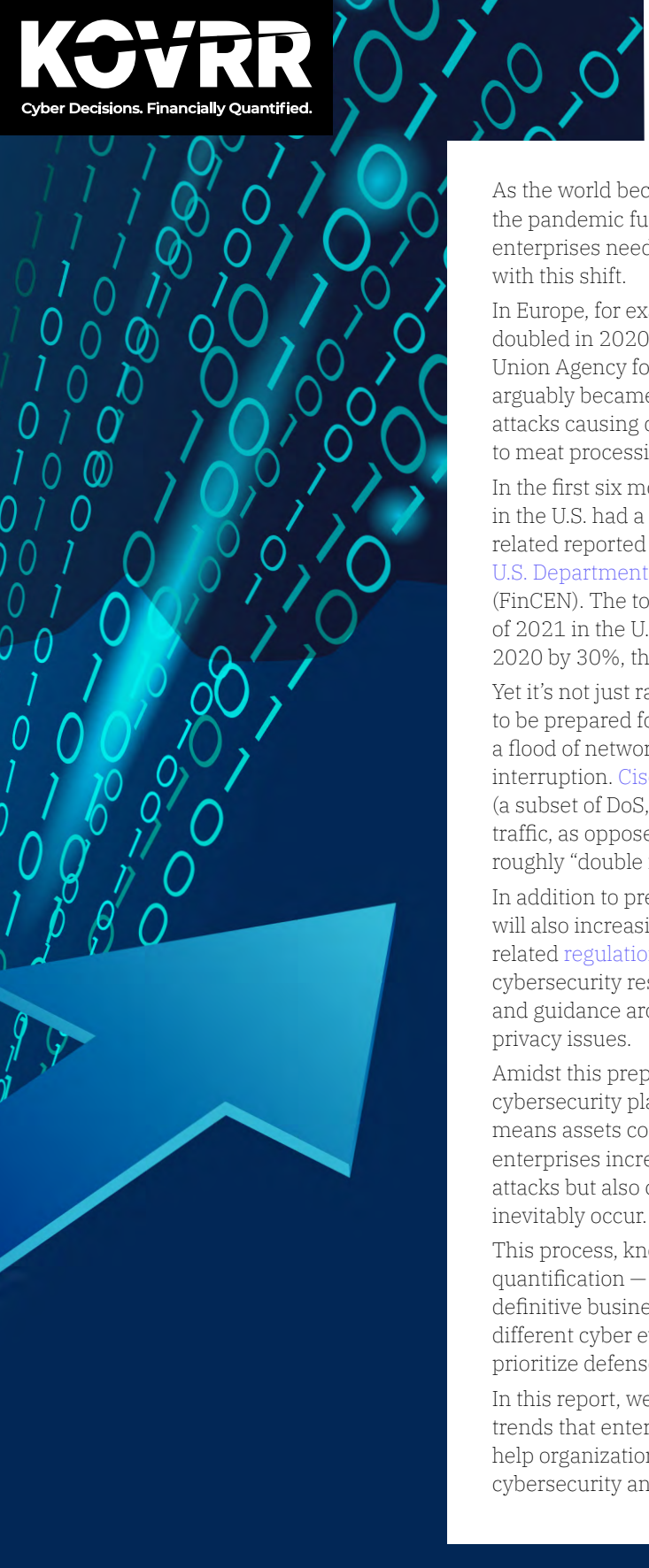
KOVRR
Cyber Decisions. Financially Quantified.

www.kovrr.com

What Emerging Cybersecurity Trends Should Enterprises Be Aware Of?

JANUARY 2022



As the world becomes more digitally connected every year — and with the pandemic further accelerating digital transformation — all types of enterprises need to be aware of the growing cybersecurity risks that come with this shift.

In Europe, for example, significant attacks on critical sectors more than doubled in 2020 compared to 2019, according to data from the European Union Agency for Cybersecurity, as reported by CNN. In 2021, the picture arguably became even bleaker around the world, with major ransomware attacks causing disruption to companies in industries ranging from energy to meat processing.

In the first six months of 2021 alone, ransomware-related reported activity in the U.S. had a higher total value ($590 million) than all ransomware-related reported suspicious activity in the U.S. in 2020, according to the U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN). The total number of suspicious events filed in the first six months of 2021 in the U.S. also exceeded all of what occurred in the country in 2020 by 30%, the agency reports.

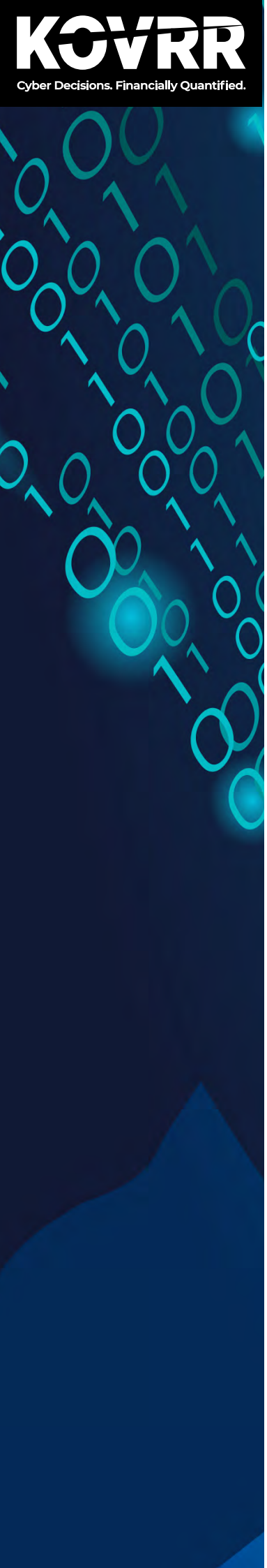
Yet it's not just ransomware that's wreaking havoc. Enterprises also need to be prepared for cyber threats like denial of service (DoS) attacks, where a flood of network activity can interrupt servers, thereby causing business interruption. Cisco predicts that distributed denial of service (DDoS) attacks (a subset of DoS, which involves using multiple devices to send a flood of traffic, as opposed to just using one device with a DoS attack) globally will roughly "double from 7.9 million in 2018 to 15.4 million by 2023."

In addition to preparing for these types of cyberattacks, enterprises will also increasingly need to be aware of and comply with privacy-related regulations. As governments around the world try to bolster their cybersecurity responses, they are passing or at least considering new rules and guidance around how companies need to handle sensitive data and privacy issues.

Amidst this preparation, enterprises also need to recognize that cybersecurity plans aren't foolproof, especially as attacks evolve. That means assets could be at risk even with solid defenses in place. So, enterprises increasingly need to think about not just how to prevent cyber attacks but also consider the dollar-value cost of risk, given that events will inevitably occur.

This process, known as cyber risk quantification — a form of financial quantification — helps enterprises think about and discuss cyber risk in definitive business terms. Knowing how much money is at stake and how different cyber events could affect revenue and profit can help businesses prioritize defenses and take mitigating action like securing cyber insurance.

In this report, we'll take a closer look at these emerging cybersecurity trends that enterprises should be aware of. Understanding these areas can help organizations potentially improve their risk management, both from a cybersecurity and overall governance standpoint.



Evolving Ransomware Risks

While ransomware is not a new type of threat, the scale and intensity of ransomware continue to broaden. Enterprises large and small, across all types of industries, need to be prepared for these cyber attacks.

For one, ransomware-as-a-service, "where ransomware variants are licensed to individuals and accomplices to execute attacks," as Reuters explains, has been on the rise. Based on suspicious activity reports, FinCEN identified 68 ransomware variants in the first half of 2021.

"The resulting emergence of new attackers has led to increased uncertainty and volatility for companies in responding to attacks due to the lack of information on the growing number of ransomware threat actors," adds Reuters.

Part of the problem is also that ransomware attacks aren't just being launched on an ad-hoc basis by individuals. Instead, there's increasingly a business-like backing behind these attacks.

"The cybercrime underground ecosystem once housed cybercriminals who would perform attacks from start to finish on their own. This one-man show has nearly completely dissolved though as one of the most prominent trends that emerged instead is the specialization of cybercriminals in different niches," notes Kela, a cybersecurity firm.

In addition to facing the more corporate structure that ransomware attackers are taking, enterprises also increasingly have to deal with the threat of state-sponsored ransomware. This underscores the growing level of sophistication in the ransomware industry, which can make cybersecurity even more challenging.

New Forms of Pressure

Not only is ransomware becoming more prevalent, but the ways in which these actors threaten enterprises also continue to evolve and expand. Instead of simply encrypting access to files and demanding a ransom to unlock this data, ransomware attackers are increasingly broadening their threats.

Cybersecurity firm Sophos identified 10 of the top tactics that these cybercriminals now use, ranging from trying to recruit insiders to help with an attack (for a share of the payout), to even physically printing out ransom notes at an affected company's location. Another major threat is that attackers will also leak data to the public or specific groups in case the ransom is not paid, which limits a company's ability to evade an attack by simply restoring data from a backup.

"Some of the tactics attackers use to coerce victims into paying are ruthless and could potentially be more damaging to an organization than a period of downtime. Attackers deliberately try to undermine their target's relationships, trust and reputation," notes Sophos.

These new forms of pressure heighten the risks that enterprises face. Even if downtime is limited, there could be additional consequences, like the loss of customers or business partners due to public notifications about the attacks.

That means enterprises need to prepare more both in terms of preventing ransomware attacks initially, as well as understanding the potential impact and how much they stand to lose if an attack does occur. The full cost of a ransomware attack can extend beyond the initial value of data that was breached to include factors like:

- The cost of mitigating the attack,
- Incident response and forensics costs
- The loss of profit associated with downtime
- Potential penalties and fines associated with sensitive data getting leaked

All these potential costs underscore why it's important to conduct financial quantification.

Facing Business Interruption and Denial of Service Threats

Another growing threat facing enterprises is denial of service attacks. In fact, that's another tactic that coincides with extended approaches from ransomware attackers, notes Sophos, such as to get hacked companies to negotiate or to distract them as a ransomware attack takes place. Even on their own, DoS attacks can be highly disruptive, and they are becoming increasingly challenging to defend against.

In the third quarter of 2021, the number of DDoS attacks globally grew by almost 24%, compared to the third quarter of 2020, according to cybersecurity firm Kaspersky. But it's not just general DDoS attacks that enterprises have to worry about. Kaspersky also found a 31% increase year-over-year in so-called smart attacks.

"These attacks are more sophisticated, often targeted, and can be used not just to disrupt services, but also to make certain resources inaccessible or steal money," explains Kaspersky.

This threat of DoS attacks can affect enterprises in multiple ways. For one, if their web host gets attacked, that can bring the company's website to a halt, which can be particularly damaging for consumer-facing sites, where their business relies on website activity. But DoS attacks can also affect businesses when vendors or other types of partners get hit, thereby potentially affecting a company's ability to operate as usual.

And as the number of internet-connected devices grows, such as with the rise of Internet of Things (IoT) devices like smart HVAC systems and connected security cameras, the risk of DoS attacks can increase too.

"The problem is that many consumer IoT devices can easily be hijacked and made part of such IoT botnets, which are then used to power bigger, smarter, and more devastating multi-vector DDoS attacks than ever before," notes CPO Magazine.

Preparing for the Worst

The good news for enterprises is that cybersecurity technology can help prevent some DoS attacks. Security company Cloudflare, for example, says it recently blocked a major attack by detecting unusual traffic. However, judging by the growing number of DoS attacks, as well as attack points, companies shouldn't assume that technology will always come to the rescue.

Instead, enterprises should have both DoS defenses as well as worst-case-scenario plans in place to deal with potential attacks.

"A proper cyber security plan includes a list of co-workers who will deal with the attack. It also outlines the way the system will prioritize resources to keep most apps and services online, which could keep your business from crashing," advises the Cloud Security Alliance. The group also suggests having a plan for contacting the relevant Internet Service Provider (ISP), which might be able to help stop the attack.

Here too, cyber risk quantification comes into play. In the event a DoS attack does occur, no company wants to be caught off guard regarding the financial implications. Ideally, an enterprise can get a sense ahead of time of what a DoS attack might cost them by using Kovrr's modeling capabilities to predict financial costs. That way, companies can take steps like setting aside a budget to deal with the fallout, as well as determining the cost/benefit of investing in various defenses.

KOVRR
Cyber Decisions. Financially Quantified.

Managing New Regulations

Another important trend to be aware of is new and emerging cybersecurity regulations. Enterprises certainly need to be prepared in terms of managing direct threats like ransomware and DoS attacks, but they also need to know what cybersecurity-related rules to follow.

For example, enterprises need to pay attention to rules around ransomware payments. While an enterprise might think that paying a ransom is the best way to resolve an attack, doing so is often discouraged by governments, and it could increasingly become outlawed altogether.

"While broader regulations may currently apply to ransomware payments, security experts should expect a more aggressive crackdown on payments. Given the mostly unregulated cryptocurrency market, there are ethical, legal and moral implications to paying ransoms, and it's vital to consider the impact of doing so," notes Gartner.

Some companies could also increasingly face higher security standards. That means enterprises not only need to focus more on how they collect and manage data to comply with regulations like the EU's General Data Protection Regulation (GDPR), but they also may have to consider rules around how they're protecting data.

The EU, for instance, is working on a new directive that will "set the baseline for cybersecurity risk management measures and reporting obligations across all sectors that are covered by the directive, such as energy, transport, health and digital infrastructure," the European Council says.

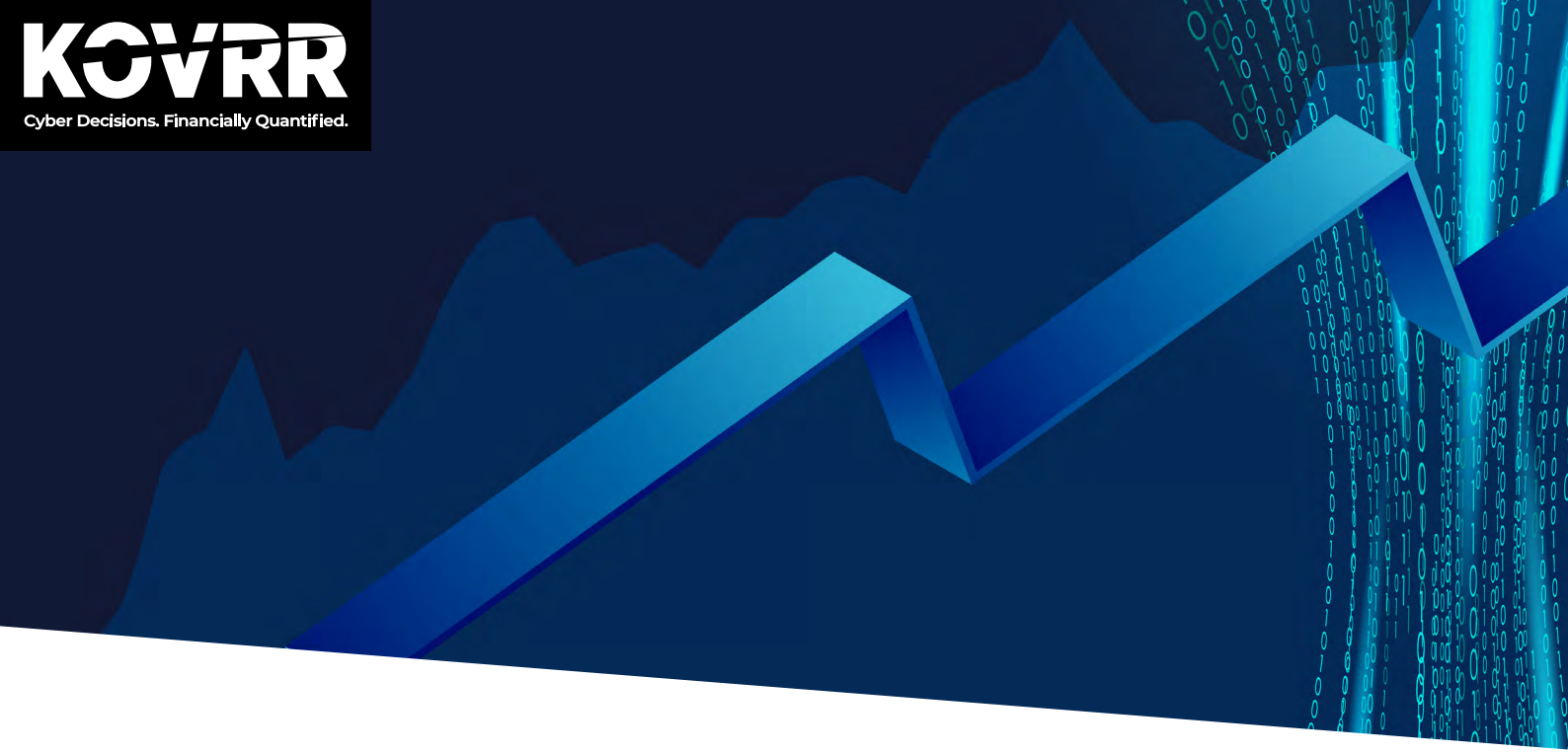
In the U.S., more reporting rules are also coming into play. For example, a new rule requires banks to report "any significant computer-security incident as soon as possible and no later than 36 hours after the banking organization determines that a cyber incident has occurred," notes the Office of the Comptroller of the Currency.

Be Prepared for What Comes Next

The cybersecurity landscape continues to change, with new threats emerging and presenting significant challenges for enterprises. At the same time, companies need to be aware of evolving data privacy rules that can affect risk management practices and incident responses.

That said, enterprises also increasingly have opportunities to leverage tools to mount strong cybersecurity defenses. Different software solutions can help prevent ransomware and DoS attacks. Some can also provide additional support, such as managing and monitoring ongoing incidents and reducing the time to mitigate once an incident occurs. Still, attacks can occur at any time, and organizations need to know what they're up against and how much it's going to cost.

Kovrr's Enterprise Cyber Risk Quantification solution helps companies gain a clearer picture of the potential financial implications they may face. Using a unique mix of global threat intelligence and financial impact data from cyber incidents, the solution can model cyber risk distinctly in business terms specific to individual companies. That helps enterprises then prioritize defenses and make better business decisions related to cybersecurity, such as determining where to invest in more defense resources and analyzing the cost/benefit of cyber insurance.



As new cybersecurity trends emerge, the solution can continuously provide real-time, actionable insights. So, rather than guessing at how new threats may affect a business, users can easily model different scenarios and get a clear sense of the potential financial impact.

> **Want to keep up with evolving cybersecurity risks more easily by getting clear, actionable business insights?**
>
> **Get in touch with Kovrr to learn how cyber risk quantification can benefit your organization.**

The Author

Shalom Bublil

CPO

About Kovrr

Kovrr's cyber risk modeling platform delivers global (re)insurers and enterprises transparent data-driven insights into their cyber risk exposures. The Kovrr platform is designed to help chief risk officers, chief information security officers, underwriters, exposure managers, risk professionals and catastrophe modelers understand, financially quantify and manage cyber risk by utilizing AI-powered risk models.
To learn more please contact the Kovrr team: contact@kovrr.com