S&P Global

Cyber Trends and Credit Risks

October 2022

Table of Contents

Introduction

Authors:
Scott Crawford, Research Director, Information Security, S&P Market Intelligence
Sudeep Kesh, Deputy Head of Analytical Innovation, S&P Global Ratings
Tiffany Tribbitt, Senior Director, S&P Global Ratings
Simon Ashworth, Head of Analytics and Research — Insurance, S&P Global Ratings
Research contributors: Manuel Adam, Zahabia Gupta, Daniel Kennedy, Nik Khakee, Thomas Zemetis

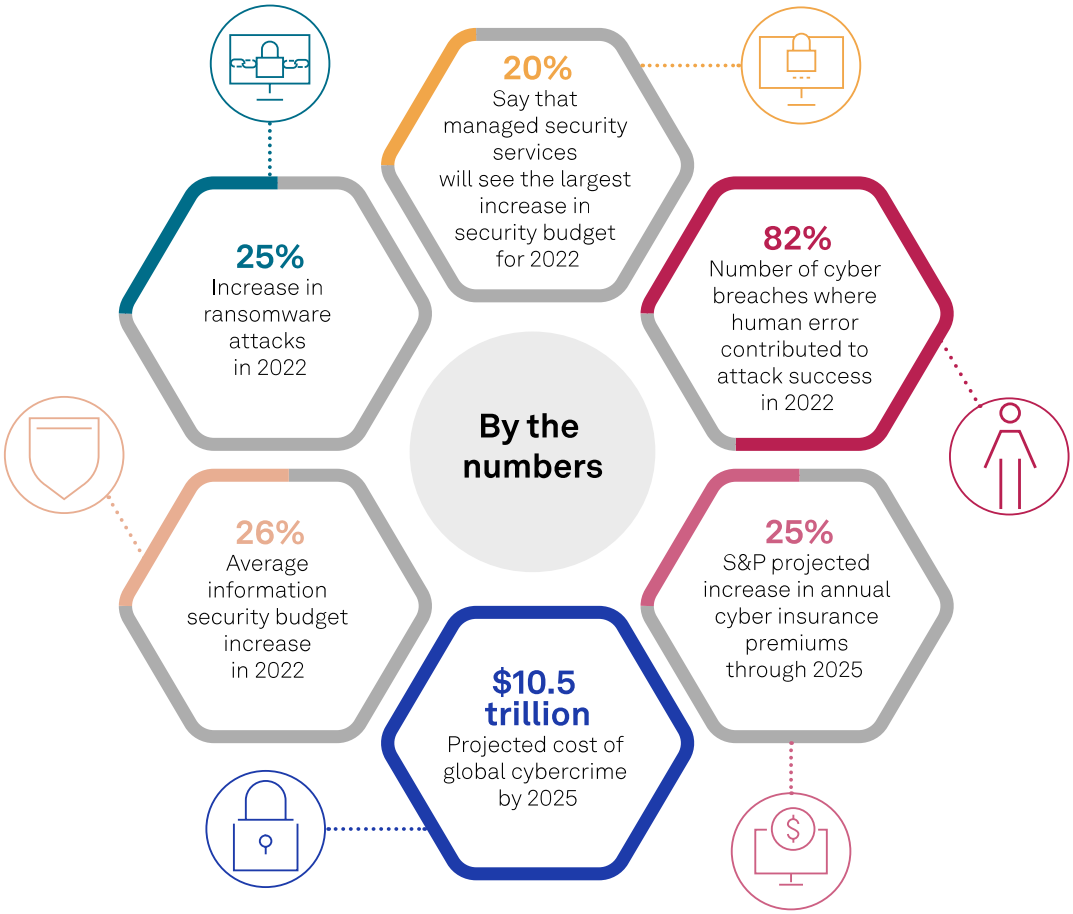
 |

Introduction

Cyberthreats are no longer an emerging risk and as such, need to be an embedded part of an entity's overall risk management profile, updated as threats evolve. While companies recognize cybersecurity is a higher priority today, roughly 40% still don't have a chief information security officer (CISO). While that may in part be a function of a company's size or complexity, for those that have CISOs, one-quarter remain on the job for just one year. The situation may be worse in many local governments, which often have fewer resources to compete for talent with the private sector and may outsource all IT needs. This underscores the challenge facing corporate, government and not-for-profit debt issuers: rising cybersecurity incidents, higher costs to combat them, and an imbalance in the executive and risk management experience needed to manage them properly. In an ever-more-connected world, the risk of systemic attacks resulting in damaging financial and reputational consequences keeps increasing. How insurers respond to this risk may also have far-reaching consequences, particularly should they move to exclude systemic attacks from claims.

Risks from cyber attacks continue to evolve, and entities must adapt to keep pace with new threats. While data breaches, ransom demands and distributed denial-of-service attacks have had limited impacts on ratings to date, the sufficiency of capital and liquidity will surely be tested for some. These trends could have significant credit implications, particularly if issuers fail to adopt proper risk management. S&P Global Ratings partnered with S&P Global Market Intelligence to explore cybersecurity trends facing the market that could significantly affect organizations of all kinds, from businesses to governments and not-for-profits worldwide.

Cybersecurity by the numbers



Sources: Verizon DBIR, 451 Research, Cybersecurity Ventures.

Threats Are Changing

Where Defenders Are Winning — and Where They're Not

As technical attacks become more challenging, attackers are targeting human nature. Although security incidents may make headlines, this often obscures the significant progress already made in defense. This has to do with the nature of the field, where attackers are always seeking to circumvent countermeasures, and defenders are constantly responding to the current attack trends. Focusing attention on where attackers win, however, doesn't fully recognize where defenders have succeeded in making things more difficult for adversaries.

Threat detection, for example, has benefited greatly from modern cloud computing environments, where providers have the scale and performance to facilitate effective advances in machine learning and analytics. Nearly twice as many respondents to 451 Research's Voice of the Enterprise: Information Security, Technology Roadmap 2022 survey say they plan to "significantly increase" their spending on security analytics, more than any other area of cybersecurity technology. Users can sign in to digital resources more easily thanks to technologies such as facial recognition and other biometric processes — technologies enabled by these same advances.

If defense has substantially improved, where then do attackers turn for opportunity? Simply put: to people. Technology is still subject to how people use it — and people can be exploited. "User behavior" is the top information security pain point, according to respondents of 451 Research's Voice of the Enterprise: Information Security, Budgets and Outlook 2022 study, and social engineering remains a popular vector of attack. The targeting of access controls is equally in play, since compromising access gets attackers inside organizations to expose sensitive digital assets. Both have been evident in recent incidents such as the Uber breach, where the adversary reportedly exploited human susceptibility in compromising controls protecting access to highly sensitive resources.

User behavior is the top infosec pain point for surveyed organizations

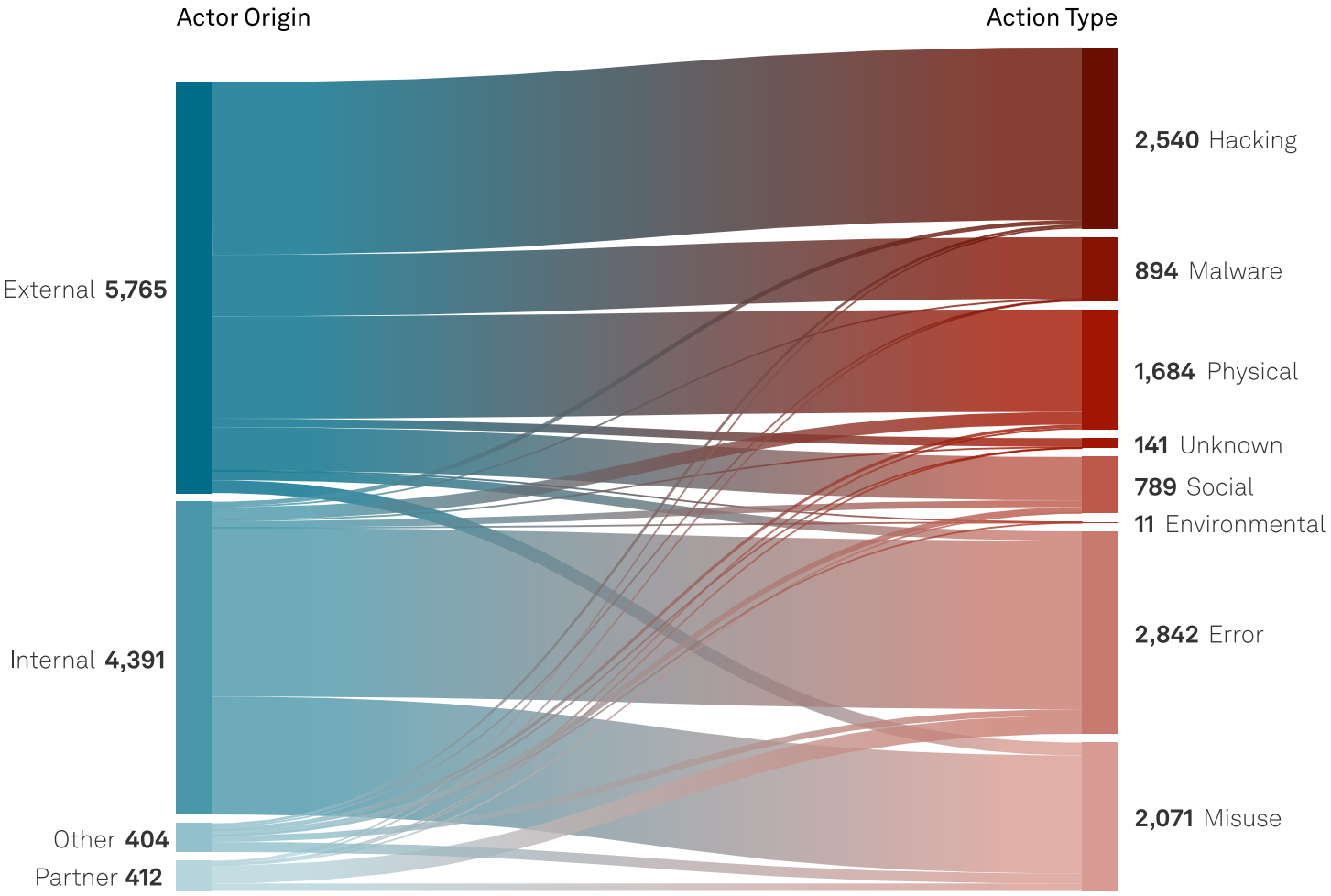
The persistence of many common exposures has been widespread enough to give rise to the industrialization of tactics such as ransomware. To be clear, cyber defense is evolving to address such threats, but as it does, they remain prevalent enough to foster the development of a well-funded underground economy, with specialization that supports complex market interactions among adversaries such as those evident in ransomware campaigns.

If we view a company's defenses as lagging or below expectations, we could lower our rating to capture this risk. We incorporate cyber defenses into our view of an issuer's overall risk management, which we consider a governance factor in our analysis. In the past 10 months, we've had just over 50 negative rating actions attributed to risk management, culture and oversight, a small subset of which were due to cyber attacks. In our experience, where cybersecurity is weak, overall risk management tends to be weaker, which could result in lower ratings than peers with similar financial metrics. Lower ratings are typically commensurate with higher borrowing costs as well as a higher incidence of default — thus, poor cyber defense and governance presents a vicious cycle for companies that could result in higher costs and reputational risks.

With cybersecurity, it is generally a matter of when, not if, an entity will be attacked — and to be prepared, issuers should take steps to mitigate these risks and adapt to a changing threat landscape. This means comprehensive staff training, cyber hygiene protocols and regularly updated response plans. Ingraining this into workplace culture and involving all staff (not just IT staff) helps mitigate the human element that so commonly leads to a successful attack.

The importance of this issue is reflected in the VERIS Community Database as illustrated below. This aligns with the 2022 Verizon Data Breach Investigations Report, which indicates that 82% of breaches investigated involve the human element, across attack types that include stolen credentials, phishing and misuse as well as error. This speaks to the degree to which attackers can exploit human interaction with technology in compromising information assets. Although comprehensive staff training and a comprehensive risk culture would help reduce the likelihood of these events occurring, they will never be totally nonexistent. Therefore, issuers should be able to promptly detect breaches and activate response plans to mitigate damage from attacks. If responses are slow or an issuer can't efficiently recover from an attack, negative rating actions may follow. In our experience, the longer an attacker is in a system undetected, the greater the likelihood of material financial damage (see "Cyber Risk In A New Era: The Increasing Credit Relevance Of Cybersecurity," published July 14, 2021 for more).

Cyber breaches by source to type



Source: VERIS Community Database; S&P Global.

Third-party vendors can both offer advantages and introduce risks. The increasing presence of cloud computing and software as a service (SaaS), not just in cybersecurity but throughout digital technology, has been one of the most transformative trends of the past 20 years. The dependency on third-party providers, however, introduces novel risks of its own.

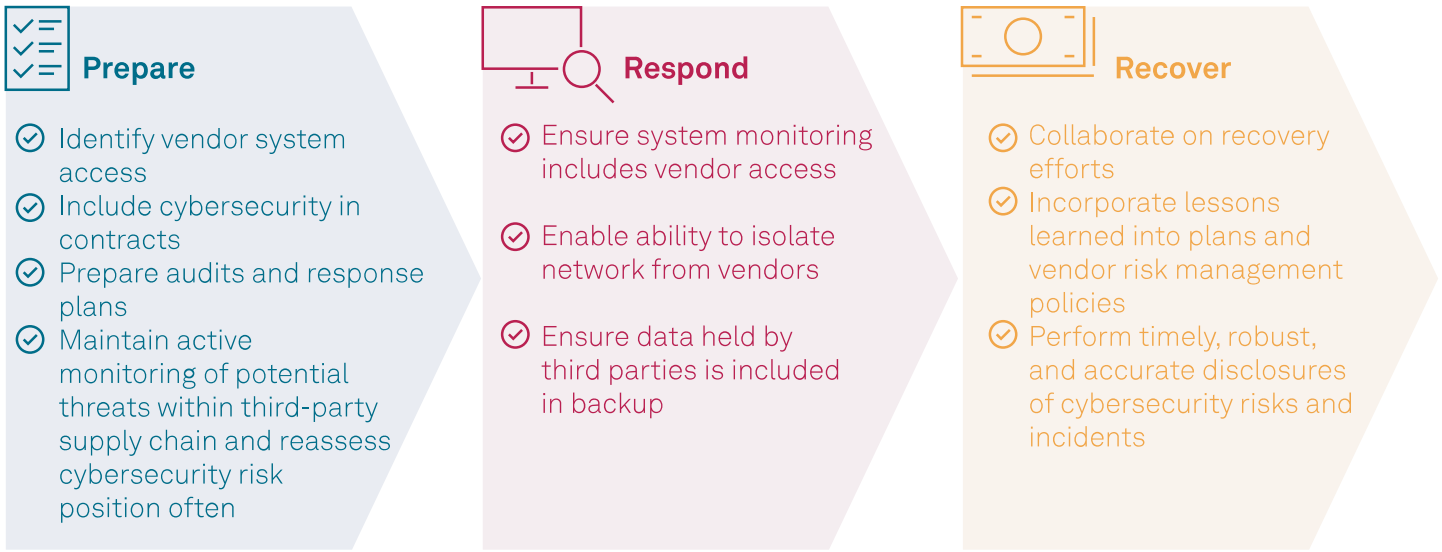
In fact, digital technology has depended on third parties for as long as organizations have used the technology products and services of others. Even conventional "shrink-wrapped" software depends on suppliers to keep their products updated against newly discovered security vulnerabilities. Today, however, that web of dependency extends in real time to the third-party services and application programming interfaces (APIs) often integrated with modern applications, which can be invoked on demand.

The nature of these risks was evident in the SolarWinds breach, which was first reported in late 2020. As a provider of IT management technology, not only was SolarWinds itself compromised, but the breach spread to many of its users as well, effectively extending the "blast radius" far beyond the company. The vast incorporation of open-source code and tool usage throughout the software landscape introduces another set of third-party risks, evident in the far-reaching impact of a critical vulnerability in a single widely used framework, Log4j, that became evident in late 2021 (see "Cyber Threat Brief: A Log(4j) Has Been Added to the Fire," published Dec. 17, 2021 for more).

These incidents further raise the question of risk concentration at key points in the "IT supply chain." To be sure, third parties offer substantial benefits. For example, just in terms of security alone, the "hyperscalers" that dominate cloud computing not only have the resources, technology and reach to leverage the most sophisticated innovations in the field, but also the potential to deploy them quickly across an extremely broad landscape. Even so, 28% of respondents to the 451 Research Voice of the Enterprise: Storage, Data Management and Disaster Recovery 2022 study reported that a cloud or SaaS failure caused their most recent outage. This highlights the need for cloud providers to keep up with the latest in cyberthreats to maintain their advantages and offset the hazards of risk concentration, which could influence client decision-making. Cloud providers have an obligation to reasonably protect their part of the underlying infrastructure. They can provide tools to users to prevent them from introducing vulnerabilities via poor configuration in the portion of the cloud they control while maintaining the flexibility those same users demand.

Strong vendor management policies are critical to limit credit impacts. We expect issuers to have third-party vendor management policies as part of their overall risk framework. An entity's security position may only be as strong as that of its weakest vendors; issuers should understand cybersecurity measures in place at major vendors, risks of unauthorized access and the need for high-quality credential standards. S&P Global Ratings evaluates how issuers mitigate their third-party vendor risks as part of our overall assessment of risk management. These are some of the key mitigants we look for:

What we're watching: key mitigants to third-party vendor risk



Source: S&P Global Ratings.

In addition to the risks posed by all issuers that engage third-party vendors, for companies such as Amazon, Google and Microsoft, given their centralized role in the cloud computing industry, we expect to see advanced security measures and leading cyber defenses due to the potential for outsized reputational damage should an attack lead to a systemic event affecting their customers.

Attackers directly or indirectly tied to sovereign actors can carry out high-impact attacks. It's not lost on military and political strategists that cyberattacks can be a powerful weapon to achieve geopolitical outcomes. Attacks on Iran's nuclear facilities via a computer worm called Stuxnet more than a decade ago signify how cyber capabilities can achieve physical damage. As we've seen in the Russia-Ukraine conflict, cyberattacks can precede or accompany military action as part of hybrid warfare, with key targets being critical infrastructure or services.

Attribution of these attacks can be problematic, allowing governments to achieve foreign policy goals, for example, by conducting espionage or disrupting services while somewhat limiting retribution and risks to reputational damage. Further, the contagion from nation-states to companies or other institutions operates with much fluidity today. We've seen this in various attacks attributed to state-sponsored actors, including NotPetya, the most

expensive cyberattack to date, according to the White House. The potential scope and scale of the impacts from a sovereign-backed attack make this threat a wild card for all issuers that could get caught in the crossfire.

In 2017, the impact of a sovereign cyberthreat resulted in substantial collateral damage when the NotPetya campaign — attributed to operatives allegedly working on behalf of the Russian military acting against assets in Ukraine — led to the spread of the attack worldwide (see "Cyber Threat Brief: How Worried Should We Be About Cyber Attacks On Ukraine?," published Feb. 22, 2022 for more). In one highly visible case, the fallout took down virtually the entire global logistics network of the major international shipper Maersk. This speaks to the potential impact of sovereign cyberthreats beyond their immediate targets, with no one inherently safe from the fallout.

Indeed, considering the extent to which IT is in the hands of the private sector, it shouldn't be surprising that private sector entities are often targeted by nation-state actors. Google and others were targeted as far back as 2009 in the campaign dubbed "Operation Aurora" by McAfee and attributed to Chinese state actors. More recently, Russian operatives were implicated in the 2021 campaign against SolarWinds and other technology vendors, leveraging their penetration of the IT supply chain to target many others.

As cyber warfare and espionage becomes more commonplace, the risks to issuers increase, particularly if cyber insurance policies won't pay. Given the motivation and resources of state-sponsored adversaries, it may become more likely that attacks will breach cyber defenses. This makes an entity's ability to respond and recover from such an attack, and risk transfer away from insurers and toward issuers, critical to credit quality. Rating actions following cyberattacks tend to be in cases where the response time significantly lagged the attacker's initial entry. The more time attackers have within systems, the more ammunition they can gain to do financial and reputational damage. Issuers such as higher education providers and research companies are targets for corporate espionage, making them vulnerable to sophisticated attacks from sovereign-backed attackers. Furthermore, court cases following NotPetya insurance claims are leading to changes in the cyber insurance market that could negatively impact policyholders expecting a payout.

The Industry and Market Are Changing to Address These Threats

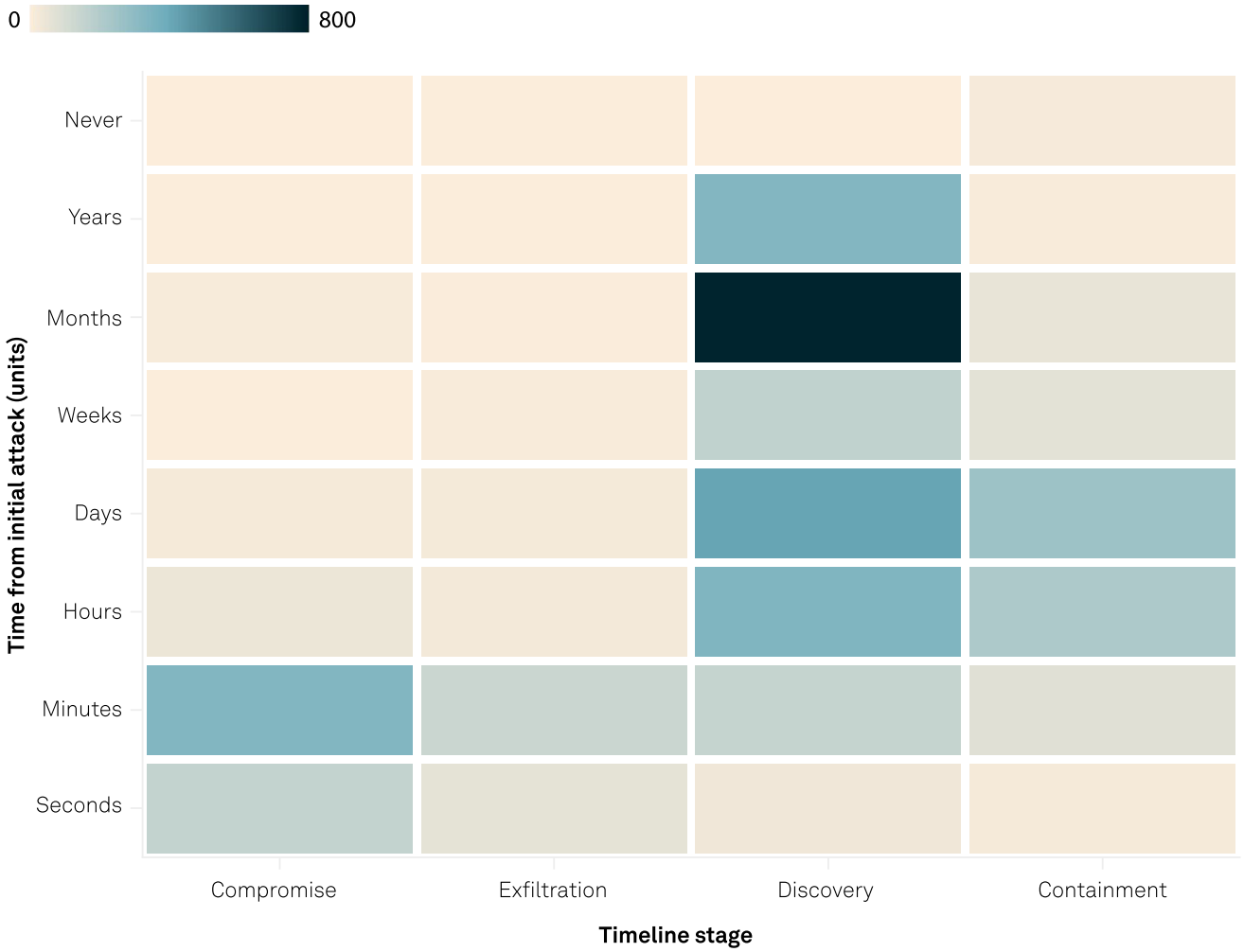
Cyber insurance continues to evolve. Beyond investing in their own cyber defenses, organizations can also consider a partial risk transfer in the form of insurance. However, the rise of ransomware, in particular, has affected the industry as a whole, while attacks that spill into the cyber realm from other fields of conflict can wreak collateral havoc, resulting in both claims and higher costs for coverage. A $1.4 billion court ruling against ACE American in January 2022 underscored the need to clarify war exclusions in cyber policies (see "Cyber Risk In A New Era: The Rocky Road to a Mature Cyber Insurance Market," published July 26, 2022 for more).

Insurers, insureds and cybersecurity technology vendors alike are partnering with cyber insurance technology vendors to help organizations implement more "insurable" cybersecurity with domain-specific expertise. Coalition, for example, saw its July 2022 valuation increase 40% over September 2021, according to S&P Global Market Intelligence. In September, it announced a partnership with cybersecurity technology vendor CrowdStrike, a company whose total revenue has grown annually between 66% and 93% for each of the past three years to nearly $1.5 billion in fiscal 2022, according to S&P Global Capital IQ Pro.

Because of the proliferation in the number and variety of cyberattacks — from ransomware where attackers strike quickly and move on to the next victim to more deliberate and stealthy operations such as espionage — many corporate executives have begun to prioritize cyberthreats, increasing resources for fighting cybercrime as well as for the growth and adoption of tools needed to protect institutions. In tandem, we've observed a decrease in response times in recent years. The illustration below shows that for the more than 500 incidents from 2012 to 2022 reported in the VERIS Community Database, it took months for organizations to discover there was an attack. More recently, organizations such as Mandiant have seen the average "dwell time" for an attack (the term Mandiant uses to measure time between initial compromise and discovery) fall from 416 days in 2011 to only 21 days in 2021, according to investigated incidents reported by Mandiant in its 2022 M-Trends Report.

This is certainly good news because the time between a cyber breach and discovery typically correlates to the level of deleterious losses for the organization. Both advancements in technology and tooling and the cybersecurity field's increased level of development have indeed helped mitigate such losses.

Organizations typically discover a cyberattack months after the compromise has taken place



Source: VERIS Community Database; S&P Global.

From a credit perspective, there are implications for both policyholders and insurers. Policyholders need to understand the risk of "silent cyber" (where policies do not explicitly include or exclude cyberattack coverage), as well as cyber warfare exclusions (through force majeure clauses), both of which could mean a policy will not reimburse costs that the policyholder might expect. For insurance companies, strict underwriting and clear policies — with precise wording — are key to the sustainable development of the cyber insurance market, especially given it is the fastest-growing subsector of the insurance market. This is highlighted by concerns about the contractual treatment of cyber warfare in the wake of the Russia-Ukraine conflict. There may be movement toward excluding systemic attacks from insured claims. However, stricter underwriting may also mean more denials of cyber insurance to protect policyholders' balance sheets, or more costly policies, potentially leaving issuers exposed to cyberthreats without sufficient liquidity to deal with the aftermath of a cyberattack.

The demand for disclosure about cybersecurity and cyber events will likely lead to regulation. Security incident disclosure has been mandated for at least as long as data breach notification laws have been in effect. In the U.S.,

breach disclosure mandates have been further extended, as with the Executive Order issued by the White House in May 2021. The SEC is also considering proposed rulemaking to expand incident disclosure for public companies.

Recent headlines have focused attention not only on disclosure, but on how security issues are revealed. Cybersecurity researcher Peiter Zatko made headlines with claims of lapses at Twitter — a company recently in the midst of a takeover controversy with Elon Musk — where Zatko had been the head of security. Meanwhile, Uber's former security chief, Joe Sullivan, has been convicted in U.S. District Court of attempting to conceal a 2016 breach through paying off threat actors under the guise of a "bug bounty," a legitimate program that rewards cybersecurity researchers for finding vulnerabilities. These events may well drive further regulatory initiatives, not only in disclosure, but in how organizations implement, manage — and disclose — their cybersecurity issues.

S&P Global Ratings relies on disclosure, but credit analysts also have direct access to issuers, often learning of undisclosed cyber events that did not have a material financial impact. This reveals the scale of the threat, but also the effectiveness of defenses. As the industry moves to standardize disclosure, greater transparency is a positive development but could also make entities with weaker cybersecurity policies more vulnerable to attacks, depending on the nature of required disclosure. It also introduces financial and governance risks associated with fines and noncompliance, as we've seen with mishandling of data following the implementation of the European Union's General Data Protection Regulation.

Cybersecurity must be an embedded part of an entity's risk management framework. The extent of these risks and the impact they have already had (and could have in the future) make considerations of cybersecurity a policy issue at the highest levels of both the public and the private sector. Lawmakers have made clear their intentions to foster a more systematic approach to mitigating risks from cyber attacks, from global data privacy regulation to executive orders on the part of national leaders, to regulators aiming to develop and enforce greater disclosure of cybersecurity incidents.

Organizations have a number of references to look to in developing their approach, from broad guidance such as the NIST Cybersecurity Framework in the U.S. to detailed practices and specifications from individual providers. The validation of adherence to accepted practices, meanwhile, has given rise to a range of providers in various aspects of risk assessment and measurement.

It's a dynamic field that is still developing, but as requirements continue to build, a consistent approach to implementation will become increasingly necessary. In July 2021, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) introduced a vulnerability disclosure platform pursuant to its Binding Operational Directive (BOD) 20-01, supporting federally mandated vulnerability identification, management and remediation. More recently, CISA issued yet another BOD (23-01) requiring that U.S. federal agencies implement automated asset inventory and vulnerability assessment. As cyberthreats continue to evolve, the effectiveness of frameworks and the nature of assessing adherence to them must adapt to changes in the threat landscape as well as in defense. As these risks — and the actions taken in both the public and private sectors in response — make clear, it has become the obligation of those responsible to the society they serve to raise cybersecurity to a strategic priority.

Cyberthreats have moved beyond a specialized aspect of risk to a near-ubiquitous priority that must be integrated into risk management frameworks. The greatest risks are the unknown unknowns. For many years, this described the cybersecurity space. However, as defenses mature, unforeseen events are more likely to be unforeseen due to poor modeling of potential risks. Issuers should frequently update their policies and practices to address changes in the threat landscape. Cybersecurity can't be the sole responsibility of the IT department or the CISO. We've seen that without proper risk management — that not only protects against an attack but also prepares for the necessary response and recovery following an attack — financial losses can compound, and reputational damage is high. Cyberattacks have led to rating changes in multiple sectors including corporates, financial institutions and U.S. public finance. As threats multiply, we expect this trend to increase.

This report does not constitute a rating action.