

Addressing the Trust Deficit in Critical Infrastructure

Global Cybersecurity
Risk Measurement and
Transparency are Key



Defending against cyber threats is a difficult task for any organization.

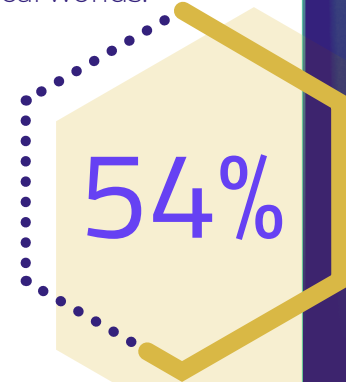
Building and maintaining trust with customers, vendors, regulators, and society at large is even more challenging.

Despite a decade or more of increased focus on cybersecurity in boardrooms, legislatures, and the media, cyber resilience is getting worse, not better. Increasing cyberattacks and highly publicized breaches have undermined the public's trust in the resilience of our societies, prompting business leaders and lawmakers worldwide to seek solutions for a mounting trust deficit.

The Fourth Industrial Revolution,¹ with its relentless pace of digitization and automation, means that organizations are becoming ever more dependent on data processing, connectivity, and business partners to deliver value to their customers and stakeholders. Those partners are creating significant cyber risk; 54% of confirmed breaches occur as a result of another organization's cybersecurity gaps.²

Threat actors exploit this growing attack surface to achieve their aims: fraud, extortion, harassment, espionage, and other harms. They are smart, adaptive, and ruthless—creating their own industry and getting rich as a result.

Organizations that suffer cyber incidents face direct and indirect costs, including business disruptions, remediation costs, reputational harms, and exposure to regulatory and liability risks. Customers and other stakeholders feel the effects of these incidents when the flow of goods and services they depend upon is disrupted, or they experience physical danger as the Fourth Industrial Revolution eliminates seams between the digital and physical worlds.



of confirmed breaches occur as a result of another organization's cybersecurity gaps.

1. "The Fourth Industrial Revolution: what it means, how to respond," World Economic Forum, January 14, 2016.
2. Report: 54% of organizations breached through third parties in the last 12 months, September 16, 2022.





Automation, for example, holds enormous promise to make automobiles much safer by eliminating the most dangerous component of a car: the human driver. The flip side, of course, is that cars are becoming more dependent on hackable components to operate safely.

For owners and operators of critical infrastructure, the stakes are uniquely high. Societies depend on these sectors for various essential services, such as energy, water, telecommunications, healthcare, and financial services. Critical infrastructure sectors rely on each other as well—energy, for example, undergirds virtually every critical infrastructure sector.

A string of ransomware attacks in 2021 affecting critical sectors in the United States and abroad highlighted the disruptive potential of the threat to a wider audience than usual. In 2022, the ransomware epidemic continued while Russia's war against Ukraine again raised critical infrastructure's profile as a target of malicious cyber activity, with Russia launching both cyber and kinetic operations against the Ukrainian energy and communications sectors in addition to military and government targets. Individually, each of these incidents caused harm to victims and their stakeholders.



Cyber Resilience is Necessary for Building and Sustaining Trust

Improving global cyber resilience involves a complex matrix of risk interdependencies that policymakers and business executives are attempting to address with laws, policies, and risk management strategies.

A key missing ingredient in many of these initiatives is an emphasis on measuring risk outcomes. After all, citizens and leaders ultimately care about organizations' resilience, not whether an organization has checked its compliance box. Resilience refers to the ability of an organization to power through adversity and "confidently pursue its mission, enable its culture and maintain its desired way of operating."³ According to the World Economic Forum (WEF),

only 19% of cyber leaders feel confident that their organizations are cyber resilient.⁴

Measurement of cyber resilience—and the trust it engenders—is an active area of innovation that policymakers and businesses alike should make a routine part of their risk management toolkits.

According to the World Economic Forum (WEF),

**ONLY
19%**

of cyber leaders feel confident that their organizations are cyber resilient.⁴

Critical Infrastructure in Crisis

Cyber incidents affecting critical infrastructure, once comparatively rare, have become much more common in recent years. Many of these incidents have involved ransomware, where the threat actor—typically a criminal group—is focused primarily on making money through extortion.

The epidemic of financially motivated ransomware attacks on health care, financial services, and government services is well-documented,⁵ but these aren't the only sectors that have fallen victim to criminal ploys. For example, the ransomware attack against Colonial Pipeline in May 2021 temporarily disrupted gas flows along the Atlantic coast of the United States. Overall, 14 of the 16 sectors considered critical infrastructure by the U.S. government experienced at least one ransomware attack in 2021, according to Federal Bureau of Investigation data.⁶

The ransomware problem is global. In November 2021, the Queensland, Australia-based CS Energy confirmed that it had fallen victim to a ransomware attack.⁷ In February 2022, a series of attacks against oil facilities in the German and Belgian port cities of Hamburg and Antwerp disrupted energy firms' operations and were likely the result of ransomware.⁸ In April 2022, Costa Rica's finance ministry suffered an attack that crippled tax and export processing services and exposed data.⁹ More recently, in November 2022, a suspected ransomware attack on a subcontractor of Denmark's national rail operator disrupted train services,¹⁰ and an attack on Vanuatu's government systems crippled the ability of that government to furnish numerous services.¹¹

5. "Internet Crime Report 2021," Federal Bureau of Investigation, 2022 (hereinafter "Internet Crime Report 2021").

6. "Internet Crime Report 2021" (2022).

7. "CS Energy hit by ransomware attack," Energy Source & Distribution, November 30, 2021.

8. "Belgium investigates cyberattack on energy companies," DW, February 2, 2022.

9. "Cyber attack on Costa Rica grows as more agencies hit, president says," Reuters, May 16, 2022.

10. "Danish train standstill on Saturday caused by cyber attack," Reuters, November 3, 2022.

11. "3 Weeks After Hack, This Country's Government Is Still Off-line," New York Times, November 28, 2022.



However, a growing number of attacks on critical infrastructure have come from nation-states and their proxies in pursuit of geopolitical objectives. For example, Russian state-sponsored threat actors have used sophisticated cyber capabilities to target a variety of U.S. and international critical infrastructure organizations, including healthcare, energy, telecommunications, and government services.¹²

More generally, Microsoft reports that the proportion of nation-state attacks, i.e., those with technological, financial, or other support from a sovereign state, against critical infrastructure doubled from 20% to 40% between July 2021 and June 2022.¹³

It's a long and growing list.¹⁴ Notable incidents recently include an attack in August against Montenegro's water infrastructure,¹⁵ Iran's September 2022 attack on Albania's government systems that brought down Albania's immigration-related IT,¹⁶ and a wave of denial-of-service attacks against Lithuania's state-owned energy company,¹⁷ to name a few. Russia is the suspected culprit behind the Montenegro and Lithuania attack.

12. "Russia Cyber Threat Overview and Advisories," Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, 2022.
13. "Microsoft Digital Defense Report 2022," Microsoft, 2022
14. "Significant Cyber Incidents," Center for Strategic and International Studies, n.d
15. "FBI's team to investigate massive cyberattack in Montenegro," Associated Press, August 31, 2022
16. "Iranian State Actors Conduct Cyber Operations Against the Government of Albania," Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, September 23, 2022
17. "Lithuania's state-owned energy group hit by 'biggest cyber attack in a decade,'" LRT, July 11, 2022.



Geopolitical Forces Compound Critical Infrastructure Vulnerabilities

A substantial part of the uptick in nation-state attacks on critical infrastructure is due to Russia's use of cyberattacks in connection with its war against Ukraine. In fact, the SecurityScorecard Threat Research team announced its discovery of a Russia-linked botnet tracked as Zhadnost in March 2022, attributing a series of DDoS attacks against the Ukrainian government and major Ukrainian banks to it.¹⁸ Researchers subsequently observed the botnet targeting the Finnish government¹⁹ and the Ukrainian National Postal Service.²⁰ Following these attacks, SecurityScorecard assessed that the Zhadnost botnet is controlled by the Russian Main Intelligence Directorate (GRU).²¹

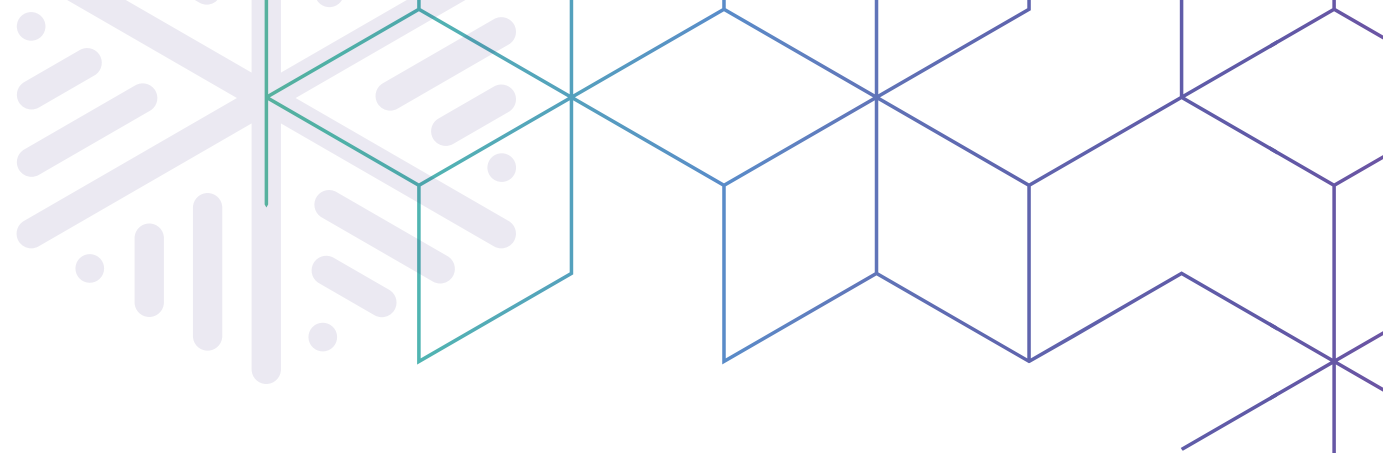
18. "SecurityScorecard discovers new botnet, 'Zhadnost,' responsible for Ukraine DDoS attacks," SecurityScorecard, March 10, 2022.

19. "Zhadnost Botnet Attacks Again: This Time in Finland," Security Scorecard, April 13, 2022.

20. "Zhadnost Targets Ukrainian National Postal Service," Security Scorecard, April 29, 2022.

21. "Zhadnost and Killnet: Distant cousins or aligned strangers?," Security Scorecard, May 11, 2022.





While attacks against Ukrainian targets have, in some cases, employed wipers capable of actual physical damage to infrastructure, those against non-Ukrainian targets have been limited to DDoS attacks by pro-Russian hacktivist groups like KillNet. On November 23, 2022 the KillNet associate Anonymous Russia claimed responsibility²² for a DDoS attack against the European Parliament's website. This occurred after the Parliament adopted a resolution declaring Russia a state sponsor of terrorism and calling upon the EU to further diplomatically isolate Russia.²³ In the months prior, KillNet claimed responsibility for attacks against U.S. state governments²⁴ and airport

websites.²⁵ A similar group,²⁶ Cyber Army of Russia Reborn, claimed responsibility for a different state government attack and another on the website of a U.S. political party's governing body. SecurityScorecard's threat assessment determined that these groups are aware of the limited and temporary operational impact of DDoS attacks but are likely to continue to conduct them due to their perceived impact on public opinion regarding the security of government institutions and critical infrastructure in Ukraine-allied states.

The approaching anniversary of Russia's invasion of Ukraine is a reason to reflect on what the conflict has suggested about threats to critical infrastructure.

Russia has long brandished its cyber capabilities against Ukraine, including a campaign of disruptive attacks in 2014 against election infrastructure, destructive attacks on Ukraine's energy infrastructure in 2015 and 2016, and the NotPetya attack in 2017 that ended up causing tens of billions of dollars in damage worldwide. In the run-up to Russia's February 2022 invasion and ever since, it has waged a relentless campaign of cyber-attacks and harassment against Ukraine, as well as attacks on Ukraine's allies.²⁷

22. "Pro-Russian hacktivists take down EU Parliament site in DDoS attack," Bleeping Computer, November 23, 2022.
23. "European Parliament declares Russia to be a state sponsor of terrorism," European Parliament News, November 23, 2022.
24. "KillNet Targeting U.S. State Government Websites," Security Scorecard, October 27, 2022.
25. "KillNet Operations Against U.S. Targets Persist with Attempted Airport Website Attacks," Security Scorecard, 2022.
26. "Russian-Speaking Threat Actors Claim New DDoS Attacks Against U.S. Targets," Security Scorecard, November 17, 2022.
27. "UKRAINE: Timeline of Cyberattacks on critical infrastructure and civilian objects," Cyber Peace Institute, June 8, 2022.





Overall, Ukraine learned from the earlier attacks and has mounted a robust defense against Russia's subsequent attempts. It's also important to acknowledge that cyber-attacks are but one capability for carrying out a given mission, especially those missions that involve generating a kinetic or another physical effect, where conventional munitions may also be used. In these cases, offensive cyber capabilities may not be cost-effective or likely to generate the desired effect in comparison to artillery, missiles, or bombs. Unlike conventional capabilities, which retain their utility against comparable targets, an offensive cyber capabilities risk exposing the underlying tools, tactics, and procedures to defenders, who may then recalibrate their network defenses to thwart subsequent use.

Russia remains a formidable threat actor in cyberspace. Ukraine is on a war-footing with Russia and fighting for its ability to exist as a sovereign nation. Its defenses are fully mobilized.

The rest of the world is not. Ukraine's allies sit in a gray zone with Russia between open war and peacetime statecraft. Russia has a proven ability to attack critical infrastructure and has frequently demonstrated its intent to carry out attacks. It almost certainly has offensive cyber capabilities in reserve. Just as worrisome, it does not necessarily need to deploy exotic, expansive offensive cyber capabilities to hold critical infrastructure around the world at risk of cyber-attacks—the sector is vulnerable.

Russia is far from the only threat actor targeting critical infrastructure. If there is money to be made carrying out ransomware attacks, cyber criminals will continue to exploit vulnerable organizations. Other nation states, including Iran, have demonstrated both the capability and the intention to attack critical infrastructure in pursuit of their geopolitical objectives.

Policymakers Intensify Focus on Critical Infrastructure

These circumstances are not lost on policymakers worldwide as governments step up their efforts to incentivize critical infrastructure with investment carrots and regulatory sticks to improve resilience against cyber risks. The first imperative for any government is to protect the health and safety of its citizenry. Market forces alone have not produced sufficient resilience against cyber threats across much of critical infrastructure; therefore, some degree of government intervention is advisable.

In the United States, explains Anne Neuberger, the White House deputy national security adviser for cyber and emerging technology, “[o]ur concerns have evolved to where we’re most concerned about degradation or disruption of critical services.”²⁸ A noteworthy carrot is the Department of Homeland Security’s (DHS) announcement in September of its implementation of the State and Local Cybersecurity Grant Program (SLCGP) and the Tribal Cybersecurity Grant Program (TCGP).²⁹ This first-of-its-kind program was established by the Bipartisan Infrastructure Law and will distribute \$1 billion over four years to help state, local, and tribal governments address cybersecurity risks, strengthen critical infrastructure, and protect their systems against persistent threats.³⁰ Congress has specified that 80% of the funds should support local governments, and at least 25% of that should be directed to rural areas.

28. “Cyber officials prioritizing securing critical sectors, foreign partnerships amid rising threats,” The Hill, October 27, 2022.

29. “State and Local Cybersecurity Grants,” Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, 2022.

30. “President Biden’s Bipartisan Infrastructure Law,” The White House, 2022.



There are no shortages of sticks in the works. Congress enacted a law in 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022, requiring critical infrastructure to report certain cyber incidents to DHS's Cybersecurity and Infrastructure Security Agency (CISA);³¹ CISA is developing and implementing regulations. Regulators as diverse as the Federal Energy Regulatory Commission, the Securities and Exchange Commission, and the Treasury Department are also in various stages of rulemaking for entities under their jurisdiction.

Globally, the EU is also pursuing two new mandates that will provide “an updated and comprehensive legal framework to strengthen both the physical and cyber-resilience of critical infrastructure.”³² The CER Directive³³ on critical infrastructure resilience is aimed at “ensuring that critical entities are able to prevent, resist, absorb and recover from disruptive incidents.”³⁴ The NIS2 Directive “strengthens cybersecurity requirements imposed on the companies, addresses the security of supply chains and supplier relationships and introduces accountability of top

management for non-compliance with the cybersecurity obligations.”³⁵

SecurityScorecard has been an active participant and contributor to policy debates about regulatory policy for cybersecurity, especially in the United States. It is imperative to improve ecosystem-wide cyber resilience capabilities by transforming how organizations measure cyber risk and act on it.

31. “Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCA) Fact Sheet,” Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, 2022.

32. “Critical Infrastructure: Commission accelerates work to build up European resilience,” European Commission, October 18 2022.

33. “Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities,” European Commission, December 16, 2020.

34. “The Commission proposes a new directive to enhance the resilience of critical entities providing essential services in the EU,” European Commission, December 16, 2020.

35. “Commission welcomes political agreement on new rules on cybersecurity of network and information systems,” European Commission, May 13, 2022.

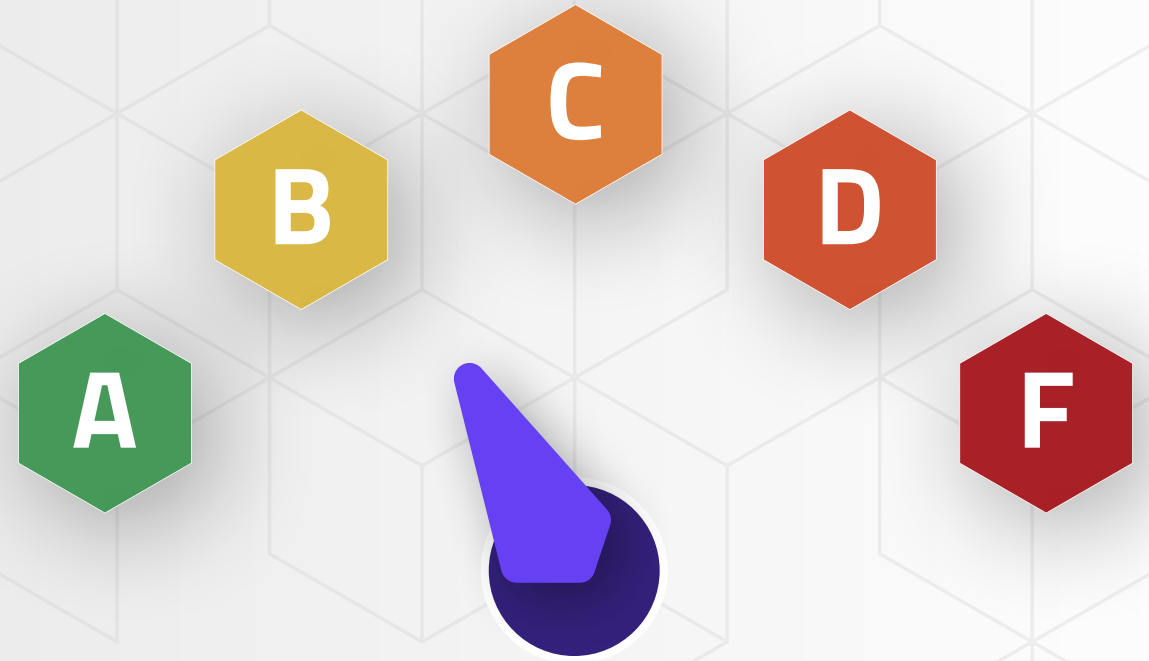


The Time is Now for a Globally Trusted Measurement of Cyber Risk

For organizations such as critical infrastructure to gain trust and build resilience, they need a simple way to measure risk and quantify the trustworthiness of any organization in the world, including partners, contractors, third- and fourth-party vendors, and supply chains. With this insight, they can identify cyber risks posed by all suppliers and make informed decisions to help their business partners strengthen their own cyber defenses.

Security ratings provide a means for objectively monitoring the cybersecurity hygiene of organizations, gauging whether their security posture is improving or deteriorating over time, and creating a viable means to improve breach defenses. Security ratings companies use a combination of data points collected externally or purchased from public and private sources and then apply proprietary algorithms to articulate an organization's security effectiveness as a quantifiable score. Adversarial intelligence has fueled the rise of security ratings by helping organizations gauge the cyber health of potential partners and vendors. With this insight, cyber insurance companies can assess risk more accurately and provide a much-needed intermediary to help build trust between the public and private sectors.³⁶ Security teams use security ratings to prioritize, understand, and implement changes to measurably improve their security posture and lower their risk of a successful breach.

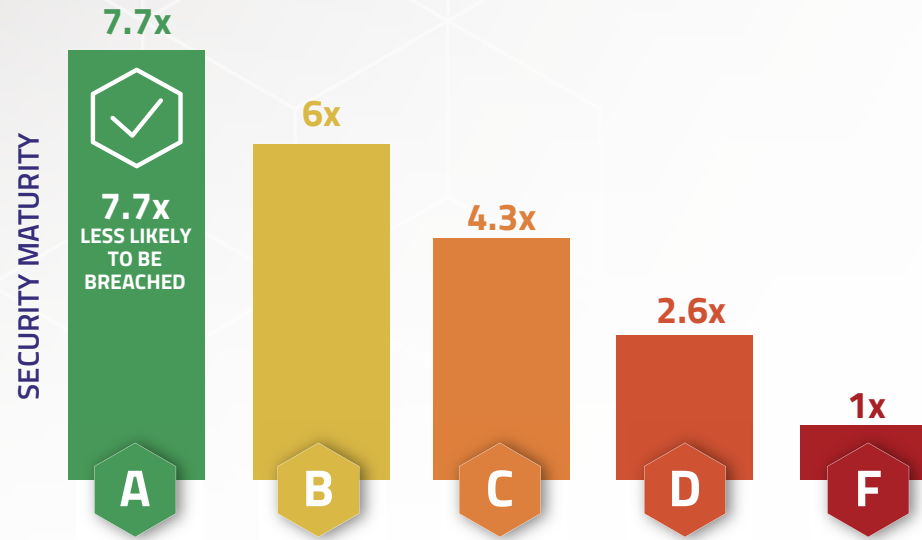
36. "How to use security ratings to build public and private trust," Securityinfowatch.com, April 2022m.
37. <https://www.cisa.gov/free-cybersecurity-services-and-tools>



Security ratings are becoming a trusted barometer of cyber resilience.

In April 2022, SecurityScorecard was added to the catalog of Free Cybersecurity Services and Tools,³⁷ established by CISA to enhance the cyber resilience of vulnerable and under-resourced critical infrastructure sectors.

SECURITY RISK MEASUREMENT, MANAGEMENT, AND PEACE OF MIND.



87% RISK REDUCTION
Up to an 87% reduction in risk by improving your score from an F to an A.



83% LESS TIME
Reduce vendor questionnaire preparation time and effort.



198% ROI
See payback from your investment in less than 3 months.

SecurityScorecard rates more than twelve million global organizations across a range of sizes, industrial sectors, and geographical locations. Analysis of this cybersecurity data allows any organization to quickly understand and continuously monitor the cyber health of their organization and those that matter to them, such as their partners, subsidiaries, peers, and more. SecurityScorecard ratings are correlated

with breach likelihood. In a recent study that utilized machine learning (ML), SecurityScorecard uncovered that organizations with an A rating are 7.7x less likely to sustain a breach than those with an F.

For bootstrapped critical infrastructure organizations, the concept of investing in more technology might seem onerous. Yet, the reality is that this technology is extremely cost-effective, especially when you consider

the catastrophic costs of a breach—for U.S. organizations, the average cost of a data breach is \$9.44 million, according to IBM research.³⁸ When considering the potential financial damages of a breach, security ratings pay off. In fact, Forrester Consulting found that customers of SecurityScorecard's measurement technology achieves payback in <3 months and offers a 198% ROI over a period of three years.³⁹

38. "Cost of a data breach 2022," IBM, 2022.

39. "The Total Economic Impact of SecurityScorecard," Forrester Consulting, May 2021.

Critical Manufacturing is a Cause for Concern



To investigate the current state of cyber resilience in the critical infrastructure sectors as designated by CISA, the SecurityScorecard team conducted a deep dive into numerous industries.

Critical manufacturing stands out as a sector that has a long way to go in terms of achieving cyber resilience. As defined by CISA, critical manufacturing includes “Primary Metals Manufacturing,” “Machinery Manufacturing,” “Electrical Equipment, Appliance, and Component Manufacturing,” and “Transportation Equipment Manufacturing.”⁴⁰ For the purposes of this report, SecurityScorecard analyzed a cohort of all critical manufacturing organizations included in The Global 2000⁴¹ Forbes list.

40. “Critical Manufacturing Sector,” Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, n.d.

41. “The Global 2000,” Forbes, May 12 2022

Forty-eight percent of companies in this sector have a SecurityScorecard rating of F, D, or C. SecurityScorecard considers 10 factors when developing an organization's security rating.⁴² When analyzing critical manufacturing further, the SecurityScorecard team found that the Patching Cadence factor experienced a significant drop across the year from 2021 to 2022, moving from an 88 (B) to a 76 (C). The Patching Cadence factor analyzes how many out-of-date assets a company has and the rate at which organizations remediate and apply patches compared to peers. This decline is likely due to an increased volume of vulnerabilities. Critical manufacturing experienced a 38% year-over-year increase in high-severity vulnerabilities. In 2022 alone, 76% of critical manufacturing organizations have high and medium-severity CVEs. These CVEs may, in some cases, facilitate ransomware groups' targeting of organizations in the sector.

Of further concern regarding critical manufacturing: SecurityScorecard's Threat Intelligence team found that the sector experienced an increase in malware

infections from 2021 to 2022. In 2022, 37% of critical manufacturing organizations had malware infections.

Ransomware groups are targeting manufacturing most frequently and, within the manufacturing sector, have attacked metal components manufacturers most.⁴³ Conti and LockBit groups are the ransomware operations responsible for the largest number of manufacturing compromises.⁴⁴

The Conti ransomware group claimed an attack against Delta Electronics. This electronics manufacturing firm supplies power components to Apple and Tesla, among others.⁴⁵ The attack reportedly resulted in the encryption of more than 1,500 of Delta's servers and 12,000 of its individual workstations, and forced it to launch a new website using a new web server while its official site was offline (presumably because its web server was one of the 12,000 encrypted in the attack).

Conti also claimed responsibility for an attack against wind turbine manufacturer Nordex SE, illustrating the potential for geopolitics to impact certain manufac-

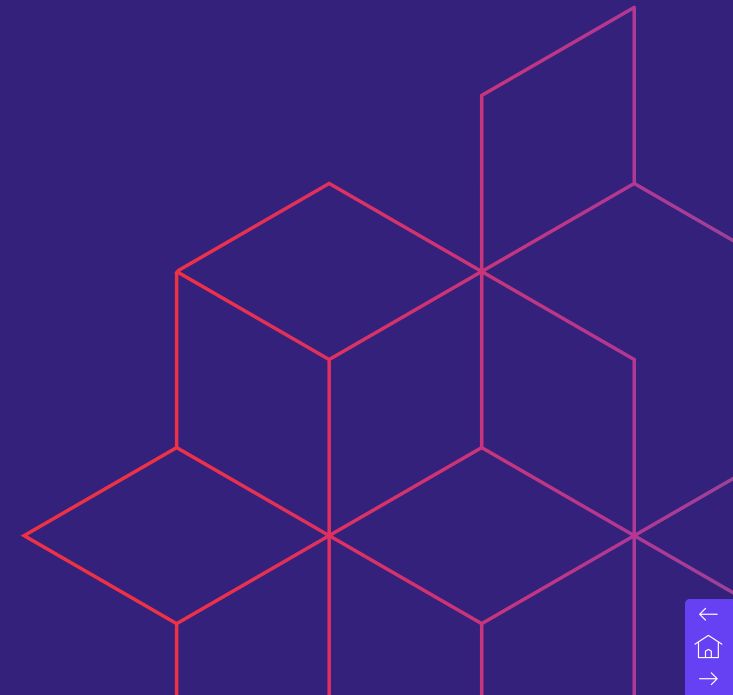
turing sectors. Conti publicly declared its support of the Russian war against Ukraine, and European manufacturers supporting renewable energy (like Nordex). The European response to Russia's invasion of Ukraine has brought renewed attention to the centrality of Russian oil and gas imports to daily life in Europe, and the attempt to reduce Europe's dependence upon those imports could drive demand for renewable energy. A subsequent investigation by the SecurityScorecard Threat Intelligence team revealed that Nordex may face ongoing risks related to the attack.

42. <https://securityscorecard.com/product/security-ratings>

43. "2021 ICS Cybersecurity Year in Review," Dragos, February, 2022.

44. "GRF Ransomware Report: Mid-Year Update," Global Resilience Federation, September, 2022.

45. "Conti ransomware hits Apple, Tesla supplier," The Record, January 27, 2022.




Trust Requires Measurement and Transparency

For decades, a common measurement methodology in IT risk management has been the color-coded stoplight scheme, where the color “green” next to a performance requirement signifies having met the requirement, “yellow” signifies partially met, and “red” signifies not met. This has never extended to the business ecosystem, which currently relies heavily on interviews with little verification.

In today's threat environment, this simply isn't good enough. Policymakers and business executives should demand greater fidelity about the security postures of the organizations that affect them, whether it's a regulated entity, their own organization, or a third-party partner (such as a supplier). Data and measurement methodologies exist that can empower leaders to understand their risk exposure and the options and tradeoffs for reducing it.

Organizations should also take steps to provide greater transparency about their level of security at their own organizations. By creating a culture of transparency, they can enhance security practices across their entire business ecosystem, raising the tide to lift all in their network. A transparent business environment also helps cultivate strong customer relationships as they will have complete visibility into what organizations are doing to protect their data and can expand business decisions beyond operational objectives to include security and risk tolerance considerations.



“Trust is at the core of the ecosystem partnerships and system-to-system relationships that exist today. An organization may feel confident or secure in their own network, within their walls, but lose faith in their ecosystem’s resilience once they have been negatively impacted by a third-party vendor cybersecurity event.”⁴⁶

46. “Global Cybersecurity Outlook 2022,” World Economic Forum, 2022.



To learn more and create
your free account, visit
SecurityScorecard.com

ABOUT SECURITYSCORECARD

Funded by world-class investors including Evolution Equity Partners, Silver Lake Waterman, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings with more than 12 million companies continuously rated. Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 30,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight. SecurityScorecard is the first cybersecurity ratings company to offer digital forensics and incident response services, providing a 360-degree approach to security prevention and response for its worldwide customer and partner base. SecurityScorecard continues to make the world a safer place by transforming the way companies understand, improve and communicate cybersecurity risk to their boards, employees and vendors. Every organization has the universal right to their trusted and transparent [Instant SecurityScorecard](#) rating. For more information, visit securityscorecard.com or connect with us on [LinkedIn](#).

SecurityScorecard.com
info@securityscorecard.com



©2023 SecurityScorecard Inc. All Rights Reserved.

