SAFE

Protecting Critical Infrastructure

APR 2022 | WHITEPAPER

Executive Summary

Michael Johnson
Board of Directors, Safe Security

This whitepaper is published at a time when critical infrastructure across the world fears a very real possibility of attack. The Russian invasion of Ukraine is evidence that a credible nation-state adversary is unafraid to increase its use of advanced cyber capabilities and that the impact will spill out into networks around the world. Organizations worldwide fear reprisal - whether fearing threats of direct attack or becoming collateral damage.

The most pertinent challenge plaguing cybersecurity of critical infrastructure is the lack of visibility of its extended, highly complex attack surface. Critical infrastructure struggles with a layered architecture that has evolved rapidly throughout the last decade, bringing the pains of information technology (IT) and operational technology (OT) convergence to the fore. As legacy technology became buried beneath newer systems, organizations began succumbing under the pressure of significant technology debt. Compound this with the increase in the frequency, impact, and sophistication of cyber attacks, the fear of losing control and access to critical infrastructure systems is keeping security and risk management leaders awake at night.

Today, boards and senior executives increasingly seek confidence in their organization's security. Businesses are pivoting towards proactive cyber risk management strategies, but they risk falling at the first hurdle: to create and execute cybersecurity strategies that are resilient by design, an organization must, first, quantify its risk. In short, if a business is not managing risk quantitatively, it could be argued that cybersecurity is not understood, and hence, not well managed.

Cyber Risk Quantification (CRQ) has never been more crucial to operating a successful global enterprise by assessing, prioritizing, and managing security risks. CRQ is key to building a healthy tension between enabling and safeguarding the business.

If you are a cybersecurity, business, or risk leader within the Critical Infrastructure industry, this whitepaper will help you initiate or augment your journey to proactively assess, prioritize, and manage cyber risk in real-time.

The State of Critical Infrastructure Cybersecurity

A historical perspective

For the better part of two decades, IT infrastructure was arguably the most significant concern for security and risk management leaders. However, as legacy systems and OT were layered with newer IT systems, security leaders struggled to create a method to maintain real-time visibility. The digitalization of businesses with the widespread adoption of cloud services prompted security leaders to reach beyond traditional on-premise cybersecurity. They did so without sufficient information on how they could best direct their finite resources. In the past, critical infrastructure organizations had two alternatives for determining the security posture of their assets:

1. Make periodic manual inventories, then input and track network devices, or
2. Deploy an agent-based solution

While the former was time-consuming and put the inventory at risk of input errors, the latter necessitated the installation of agents on each network device that would quickly get outdated, requiring a reinstallation.

Network monitoring is an important initial step in such a scenario, but it is insufficient to combat the new and developing security threats that explicitly target the critical infrastructure industry. **Businesses require complete insight into their entire operation, including their people, processes, ICS environment, converged IT/OT infrastructure, cybersecurity products, and third party (*nth*) vendors**

VULNERABILITY ADVISORY FINDINGS

More than twice as many common vulnerabilities and exposures (CVE) were published in 2021 than in 2020.

38% of ICS vulnerability advisories contained errors that would make it difficult to prioritize mitigations.

35% of the advisories could cause both a loss of view and loss of control in OT systems.

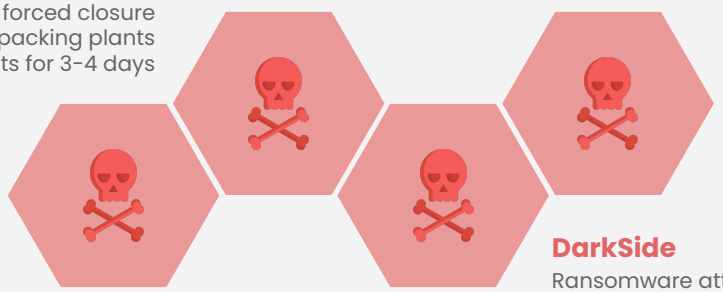
19% of advisories without a patch had no alternate mitigation.

Source: 2021 ICS OT Cybersecurity Year In Review - Dragos 2021[1]

Critical Infrastructure during current times of conflict

Although the land invasion of Ukraine took place on February 24, 2022, a deliberate, systematic campaign of advanced cyber attacks on its government and critical infrastructure is reported to have begun much earlier. At the time of writing, the repercussions continue to cross the chasm of land and virtual warfare beyond legal, geographic, and economic boundaries. **Critical infrastructure has been the prime target even prior to the current conflict.**

NOTABLE ATTACKS ON CRITICAL INFRASTRUCTURE



REvil
Ransomware attack forced closure of 5+ major meat packing plants across 3 continents for 3-4 days

ITSec
State-sponsored attack on Bowman Dam, New York, enabled adversary to manipulate SCADA controllers.

LightBasin "UNC1945"
Harvested data from at least 13 telecommunications companies between 2019-2021.

DarkSide
Ransomware attack on a major US fuel pipeline, and two German plants lost control of their tank loading and unloading processes

SAFE

These events demonstrate strong intent to target industrial organizations by acquiring access to industrial control systems and operational technology networks. **Organizations are unable to fully manage the volume of security threats coming at their most valuable assets - people, processes, technology, and third parties.** This presents a series of vital challenges to overcome:

1. **Tackling past, present, and future: IT, OT, and the Internet of Everything:**
   - The rapid expansion of digital technologies, interconnected devices and systems, and company growth has resulted in legacy, shadow infrastructure, and processes, creating costly technology debt
   - The competitive opportunities of cloud computing and big data vs. successful migration, adoption, and maintenance
   - Rethinking security to address IT/OT convergence with finite resources; a shortage of time, talent, and financial investment

2. **Third party risk: assessing and managing immediate, external risk:**
   - 100% of Food & Beverage, 77% of oil & gas, and 75% of water utilities architectures have external connections to OT[1]
   - 63% of organizations do not possess visibility into the level of network access and permissions for internal or external users[2]
   - Organizations have a limited-to-no understanding of who, or what, has what permissions and access, and why.

3. **The growing sophistication of adversaries: from rogue individuals to well-funded, driven, nation-state capable organizations:**
   - Adversaries are launching systematic campaigns and performing planned reconnaissance. The Conti group's private chats reveal a hierarchical structure complete with strategies for growth, expansion, and hiring.[3]
   - Advanced TTPs see attackers lying in wait within the interconnected systems of businesses to cause malfunction, extort ransom, or destructively eliminate resources.

Why is the spotlight on critical infrastructure cybersecurity now, when the problems have persisted for so long?

Truth is, the spotlight never dimmed - though more people are taking notice.

> *"Most of America's critical infrastructure is owned and operated by the private sector, and critical infrastructure owners and operators must accelerate efforts to lock their digital doors… If you have not already done so, I urge our private sector partners to harden your cyber defenses immediately by implementing the best practices we have developed together over the last year."*
>
> – President Biden *March 21, 2022*

The question of risk is at the forefront of any conversation. **85% of critical infrastructure in the United States is privately owned.** As Cybersecurity and Infrastructure Security Agency (CISA) outlines[4] in its 'Shields Up' guidance, **"the first step to resilience is to reduce the likelihood of a damaging cyber intrusion."** However, to reduce the likelihood of an incident, an organization must be well managed in security, which first requires the quantification of its likelihood of happening – an organization's cybersecurity risk posture.

The debate of immunity versus resilience against cyberattacks will **always lean towards resilience**: *It is not 'if' but 'when' a breach may occur.*

Building cybersecurity that is resilient-by-design requires visibility

Critical infrastructure organizations are beginning to look beyond their physical, on-premise cybersecurity risk to gain true visibility of cybersecurity risk across an enterprise. There is more that businesses can do to adopt **proactive cybersecurity**. Increase resilience by thinking beyond detection and response of advanced persistent threats (APTs), malware, ransomware, DDoS, network attacks, code flaw vulnerabilities, and privilege escalations. **Most organizations already have the data to embrace proactive cybersecurity using the services and initiatives that exist across the estate.**

a. **Implement information and technology management best practices:**
This seems an obvious first step towards building a cyber-resilient organization, but the 2020 Data Risk & Security report reveals that 54% do not follow basic security practices such as reviewing user access rights to data regularly.[5] **Make an effort to adhere to and continuously monitor IT management best practices**, including network segmentation, multi-factor authentication, network access control, and more.

b. **Actively promote and practice information sharing and mutual defense.**
Both public and private sector organizations share information and cyber defense best practices in critical infrastructure communities of interest, such as the Information Sharing and Analysis Centers in the United States.[6] **Encourage your security teams to stay abreast of updates and utilize valuable industry resources such as the MITRE ATT&CK Framework to identify potential risks** within your organization and how to mitigate them.

c. **Quantitatively assess, prioritize, and manage risk**
All businesses are trust-based, digitally-native businesses, and given the threats businesses face today, this gives CISOs and CIOs the toughest executive roles. Employees, policies, technology, and third parties – every aspect of a company poses a cybersecurity risk. The consequence of being ill-managed with cybersecurity results in firefighting and reactively addressing one crisis after another. **A better state of preparedness and resilience will always result from a proactive and quantitative approach** to cybersecurity.

Why is a quantitative approach significantly better?

It creates transparency and accountability within leadership.

Being able to communicate cybersecurity to the board is an age-old pain point. Cyber Risk Quantification helps security leaders to enable those who own the risk (CEO, Board, the business, and relevant stakeholders), and those who manage the risk (CTO, CIO, CRO). Where other solutions fail, it succeeds in **bringing risk governance and management together.**

> *Today, infrastructure such as healthcare systems, power grids, transportation, and other critical industries are increasingly integrating their operational technology with traditional IT systems to modernize their infrastructure, and this has led to new vectors of cyberattacks. Though businesses are ramping up their security initiatives and investments to defend and protect, their efforts have largely* ***been siloed, reactive, and lack business context. The lack of visibility and proactive cyber risk management is a major challenge for critical infrastructure.***

Organizations that effectively manage their cybersecurity risk share one common characteristic: they each take a proactive approach. They understand that managing cyber risk requires quantification and prioritization against threats faced. **By quantifying risk, organizations proactively move to a position of understanding and gain an invaluable capability - taking the guesswork out of cybersecurity.**

The Key Benefits of Cyber Risk Quantification

Become proactive

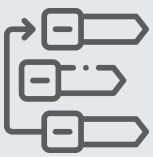
Use a data science-backed risk prediction engine to know which threats are most likely to cause a data breach. Measure, manage, and mitigate risks before breaches happen.

Improve efficiency

Know the ROI of your cybersecurity investments. Automate cyber risk management and eliminate the manual monitoring of multiple applications & platforms.

Remove silos

Get an integrated, real-time view of your cyber risk across people, processes, technology, cybersecurity products, and third parties, with the one score that matters.



Prioritize actionable insights

Redirect your finite resources to accept, mitigate, or transfer the risk based on your cyber risk appetite. Revisit your cyber insurance coverage to secure fair premiums.

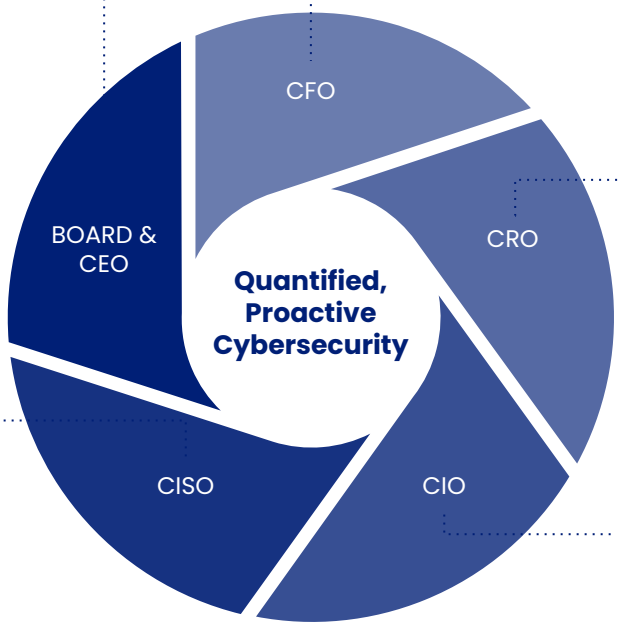
Contextualize cybersecurity communication

Produce board-ready reports and the financial impact of a data breach. Communicate cyber risk in a language the board understands.

Cyber risk quantification helps you answer the biggest questions in cybersecurity

CFO
How **efficient is our cyber insurance coverage**? Have we adequately deployed risk-sharing methods against direct and indirect cyber attacks that may affect the business?

Board & CEO
What is the **impact of a cyberattack** on people and its global economic implication? What are we doing to reduce the impact of cyber events; financial and otherwise?



CRO
How can we **maximize cyber risk burndown** with efficient investments? Is our cyber insurance coverage and premium as per our cyber risk appetite.

CISO
What is the risk across people, processes, technology, and third parties? How do I **justify cybersecurity initiatives** and **communicate cyber risk effectively**?

CIO
How are we managing risk across the enterprise and crown jewels? How are we **prioritizing mitigation strategies**?

At a time of 'everything' shortage across industries - time, talent, and budget - security and risk management executives need to be prudent and cautious of where they direct their finite resources.

Learn how Cyber Risk Quantification helped this Fortune 300 healthcare organization leverage data and remove emotion from their cybersecurity decision-making process.

Conclusion

Quantify risk to better protect your organization

Traditional approaches to cybersecurity do not actively manage cybersecurity risk. Organizations today require a cybersecurity risk management solution that maintains a healthy tension between enabling and safeguarding businesses.

The recent Strengthening American Cybersecurity Act of 2022 passed by the United States Congress places specific legal requirements on its federal agencies to disclose incidents and attacks and mandates its Cybersecurity and Infrastructure Security Agency (CISA) to perform continuous assessments of federal risk posture.[7]

As a business concerned about cyber resilience and maintaining a strong cybersecurity ecosystem, you have stores of valuable data at your fingertips. What's missing is the method to pool this information, identify risk, and leverage sound data-science-backed technology to quantify that risk. It is this technology and rethinking of risk management that will enable you to take a smarter approach to cybersecurity - choosing measured and informed prioritization of risk over guesswork and hoping for a favorable outcome.

This powerful capability cannot be built in-house overnight

Safe Security has used its years of experience in cybersecurity and developed a platform built by experts, including a collaboration with MIT to produce a unique Bayesian algorithm. We recognize the urgency of giving organizations a powerful cybersecurity risk quantification platform with sound data science-backed principles, automated deployments, and agility to adapt to newer technologies in near real-time. Cyber Risk Quantification gives security teams, corporate executives, and board members alike visibility, confidence, and proof that an organization is using its time, energy, and resources to effectively manage cybersecurity risk and contain risk exposure.

British Telecommunications, BT Group, is the United Kingdom's leading telecommunications and network provider and one of the largest global communications services and solutions providers, serving customers in 180 countries. They use cyber risk quantification to their advantage as customers and investors in Safe Security. The investment allows BT to combine the SAFE platform with its world-leading managed security services to provide customers with a real-time view of how safe they are against an incredibly fast-moving cyber threat landscape.

"Adding SAFE to BT's proactive, predictive security services will give customers an enhanced view of their threat level and rapidly pinpoint specific actions needed to strengthen their defenses. Already one of the world's leading providers in a highly fragmented security market, this investment is a clear sign of BT's ambition to grow further."

Philip Jansen
Chief Executive of BT

About Michael Johnson

Michael serves on the **Board of Directors of Safe Security** which focuses on quantitative enterprise cyber risk measurement. Michael serves as the **Chief Information Security Officer (CISO) for Meta Financial Technologies**, Meta Platforms, Inc., overseeing security for all of Meta's payments and financial services. Previously Michael served as **Capital One's CISO and Senior Vice President**, leading and managing information security, cybersecurity operations, and security technology innovation. Prior to joining Capital One, Michael served as the **Chief Information Officer (CIO) for the U.S. Department of Energy**, and in other key cyber-focused executive roles in the U.S. Government at the **Office of the Director of National Intelligence**, the U.S. **Department of Homeland Security**, and the White House **Executive Office of the President.**

About Safe Security

Safe Security is a pioneer and leader in **"Cybersecurity and Digital Business Risk Quantification" (CRQ)**.

It helps organizations **measure, manage and mitigate enterprise-wide cyber risk in real-time** using its **ML-enabled API-first SAFE platform** by aggregating **automated signals** across people, process and technology, for first & third-party to **dynamically predict the breach likelihood (SAFE score), recommend prioritized actionables & provide the $ risk of data breach to an organization.**

References

1. ICS/OT Cybersecurity Year in Review, 2021, Dragos Report 2022
2. A Crisis in Third-Party Remote Access Security, Ponemon Institute Report 2021
3. Burgees, M. (2022, March 16). The Workaday Life of the World's Most Dangerous Ransomware Gang. Wired.
4. Shields Up, CISA
5. Netwrix Survey
6. National Council of ISACs
7. Proposed rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

Palo Alto
3000, El Camino Real,
Building 4, Suite 200, CA
94306

www.safe.security | info@safe.security

Palo Alto • New York • Dubai •
London • New Delhi • Singapore

SAFE is SOC 2 Type 2 Certified | AICPA