PONDURANCE

# Cybersecurity Predictions for 2022

pondurance.com

# Introduction

Predictions are predictably unreliable, but one thing is certain: cyberattacks will continue to challenge organizations in 2022 and potentially disrupt our everyday lives. Indeed, the United Nations has reported that cybercrime is up 600% due to the COVID-19 pandemic—and now nearly every business is being forced to adapt and evolve.[1] In this eBook, we share top emerging trends we are seeing that could shape the cyber industry in the coming year.

1

# Going back to the risk management drawing board


Any successful cybersecurity program is predicated on a thorough risk management approach. The strategic element as of late seems to have been relegated to a fragmented set of tactics and solutions, as companies find themselves in a more reactive than proactive mode when protecting assets.

In order to efficiently allocate their security budgets, consolidate existing technologies and harmonize control procedures across a vastly extended network, we will see more companies revisit their risk management program. For instance, legacy mitigation has largely relied on a third-party, risk transfer approach, which means organizations will have to more directly consider downstream impacts that may have intolerable business impacts on their operation.

We're already seeing an increase in the rigor toward vendor management programs to confirm the level of due care, and increase the level of accountability. At Pondurance, we conduct risk assessments based on the NIST Cybersecurity Framework to examine the most critical aspects of your environment. We provide valuable insights into an organization's cyber-risk levels and recommendations for mitigation.

Increasing the rigor of risk management will properly define systemic risk, putting organizations back in the **DRIVER'S SEAT.**



PONDURANCE

2

# The hybrid workplace will be the next frontier for cyber

Organizations will have to learn to mitigate the risk of cyberattacks while juggling the constantly changing demands of both on-site and remote workers. In the wake of the COVID crisis, some companies went from zero to full digital transformation overnight. Other companies are still on that path.

Regardless, now that some employees are returning to the office and others remain at home, companies will need to ensure that workers remain productive and secure in this new hybrid environment. Hybrid work will require a complete overhaul of how we think about security, including the ability to provide employees with easy and secure remote access to business-critical applications no matter where they are.

Increase **AWARENESS, FLEXIBILITY AND CONTROL** while catering to a geo-flex workplace environment.



PONDURANCE

3

# Governments will put the squeeze on cyber syndicates

Governments around the world will really clamp down on cybercrime. Cybercrime is a global problem, and world leaders want to establish norms when dealing with this type of crime. Expect to see more cybercrime legislation around the globe to put the squeeze on cybercrime syndicates and make it harder for them to evade police action.

This could include new laws that make it easier for police to gain search warrants, as well as more anti-corruption legislation to disrupt the use of cryptocurrency in cybercrime. Though cybercrime syndicates are still emerging, we predict at least one major cyber ring will be shut down this coming year.

In no small part, the current administration is likely to use the power of embargoes and other economic tools to better drive cross border law enforcement.

The government will avidly pursue bad actor groups, but **ONGOING DILIGENCE IS KEY** as the vacuum will be quickly filled by other opportunists.



PONDURANCE

4

# The Cybersecurity Maturity Model Certification will extend beyond the DOD


The Department of Defense (DOD) recently set up a process to ensure that all defense contractors meet certain requirements for handling controlled unclassified information. That process is known as the Cybersecurity Maturity Model Certification (CMMC). It is designed to ensure that defense contractors meet a basic level of cybersecurity hygiene for protecting sensitive information.

It's fair to predict that not only will DOD suppliers need to meet the cyber hygiene requirements, but that the same kind of compliance will soon be required across all government agencies and their suppliers. Why? Because a government agency breach could have a major impact on the lives of average citizens. The Department of Homeland Security, for example, is already exploring options for creating a cybersecurity standard for contractors.

At Pondurance, we know that meeting CMMC requirements can be challenging and as a registered provider organization, we can help prepare for your assessment.

The need to provide security assurance is **BECOMING LESS OPTIONAL**, particularly for service organizations that process, store or transmit sensitive data.



PONDURANCE

5

# Cloud customers will need MDR for greater protection

The cloud can be just as insecure as any on-premises data center, especially given misconfigurations and the typical cyber hygiene problems that plague most companies. When moving to the cloud, organizations need to appreciate the fact that they have a shared responsibility to protect their corporate data along with their cloud service providers.

As a result, there will be a greater need for managed detection and response (MDR) to better integrate with the cloud. Next-gen MDR offers an effective solution for cloud computing security by providing broad threat defense, such as filling detection gaps and automating responses to evolving threats.

MDR can be an extension of your security team or act as your security team. The security operations center that you gain from an MDR is on 24/7 and can act on alerts to ensure that your environments, both cloud and on-premises, are protected from bad actors.

Dynamic security for the cloud is **ESSENTIAL TO PROPERLY FOSTER PROTECTION** of your extended network.



PONDURANCE

6

# Humans will matter more than ever

When it comes to cybersecurity, you can't rely strictly on automation. But a lot of companies do. They believe that humans can be removed from the cyber equation and replaced with AI and automation technology. While there's no doubt that automation is getting better, it is unlikely to reach a level of maturity to truly remove humans in anyone's lifetime that is reading this.

Of course, automation is necessary for managing certain processes and correlating disparate events. But to find and mitigate nefarious attacks, human involvement is just as critical as the latest and greatest security tools. Cybercriminals are humans and you need human defenders to combat human attackers.

Companies should never forget about the importance of the human element in detecting and deterring threat actors. In the coming year, human intervention can be the difference between swift containment and grave consequences.

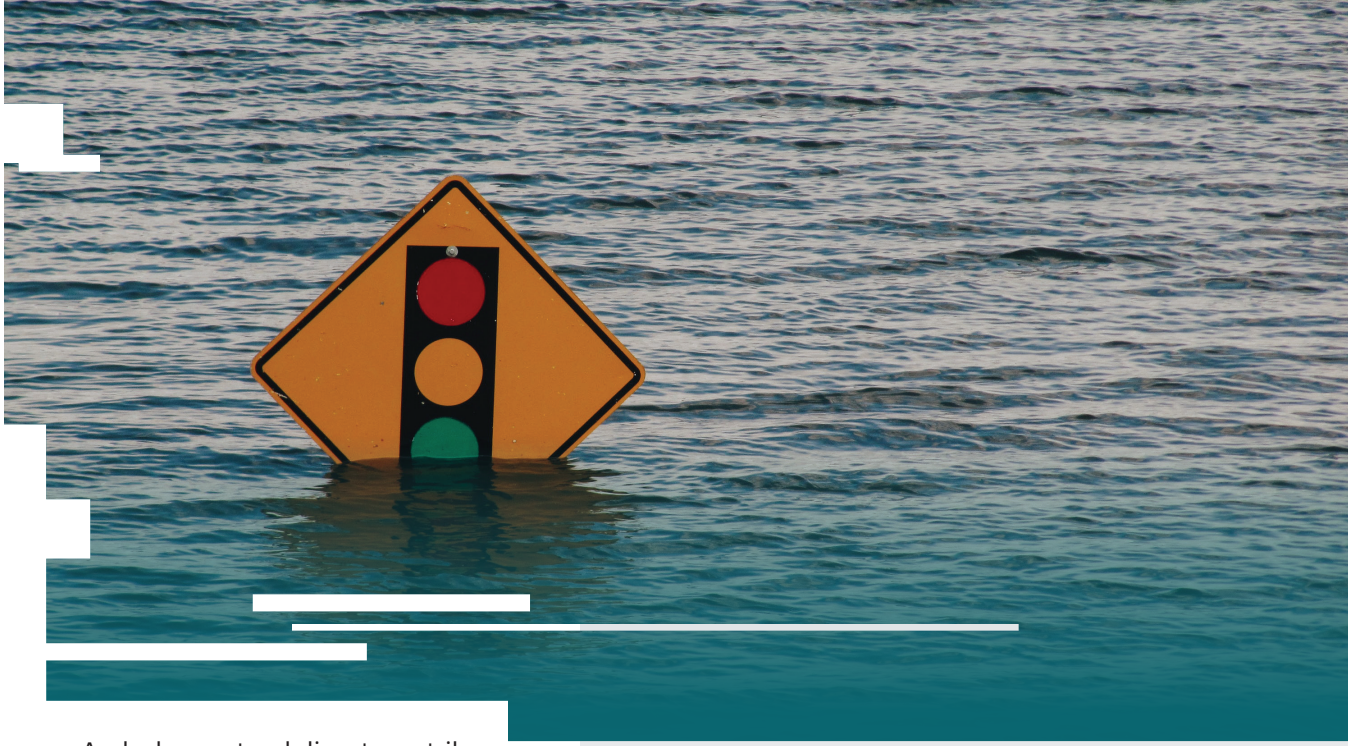
Humans remain both the **GREATEST ADVERSARY** and the **GREATEST POTENTIAL EXPLOITATION PATH** where critical infrastructure and sensitive data assets are concerned.



PONDURANCE

7

# Natural disasters will bring increased cyber risks



Natural disasters like hurricanes, wildfires, earthquakes and floods are increasing in size and frequency. And when natural disasters strike, communities and organizations are the most vulnerable. Cybercriminals understand this—and they will make it a priority to take advantage of environmental events to create more havoc by targeting physical infrastructure like electric grids, fuel pipelines and water systems with ransomware attacks.

Businesses, state and local governments must respond to this growing threat by better preparing their defenses and regularly running disaster drills and simulations to counter these threats. The more they practice, the better their response will be.

At Pondurance, we joined forces with the Indiana National Guard who conducted a drill at Muscatatuck Urban Training Center in Indiana, to test preparedness and bolster defenses. This drill involved a simulated earthquake followed by a cyberattack, with bad actors swooping in amid the chaos and attacking the water system to try to shut it down as the National Guard deployed its defense tools to protect networks, people and property. We also participated in a workshop for water and wastewater utilities in a red team / blue team cyber simulation event in another effort to bolster defenses by sharing knowledge.


Cybercriminals are opportunists that **THRIVE ON CHAOS**, often using the distraction of a kinetic event to increase the success of their cyber exploits.

8

# Cyber insurance will be harder to get

Cyber liability insurance is a type of insurance designed to cover losses and penalties associated with a data breach or other cyberattack. But this kind of insurance will become harder to get. Why? Because for the first time, ransomware has hit a level where the payouts by insurance companies are now exceeding the premiums being paid. That means large insurance providers could limit the amount of business they book and be very selective when it comes to underwriting new cyber policies.

Some cyber insurance providers are even excluding ransomware coverage when they renew customers. Businesses will have to up their investments in cyber tools, processes and staffing to prove to insurance providers they are a worthwhile risk.

Cyber liability insurance is no longer a boutique product; you must now **PROVE YOU ARE "INSURABLE"** based on your level of cyber readiness and due diligence.



PONDURANCE

9

# Nation-state attackers will expand their disinformation campaigns

Nation-state attackers will target the U.S. economy and financial institutions with disinformation, much like they have targeted our political institutions. These nation states could spread misinformation about the viability of our banking system, thus stoking panic among consumers and causing a run on our banks. These campaigns will be small in nature, but they could add up to make people lose confidence in our financial systems.

Information will continue to be **WEAPONIZED BY NATION STATES** with even greater precision and effect to influence the outcome of national events.



PONDURANCE

10

# High schools and trade schools will start to train the cyber workforce

The search for cyber talent will continue to be front and center. The cybersecurity industry is currently short about 3 million qualified workers, according to the latest (ISC)² Cybersecurity Workforce Study, and this shortfall is tipping the balance in favor of the bad guys.[2] To help level the playing field, we will start to see more educational programs geared toward cyber, including the rise of trade schools with specialized degrees, as well as more high school programs that are focused on cyber skills.

Companies will realize that they can hire talent directly from high schools and trade schools, and that cyber workers of the future don't necessarily need a four-year college degree to enter the field.

This should help with the shortage of skilled workers needed but will take some time!

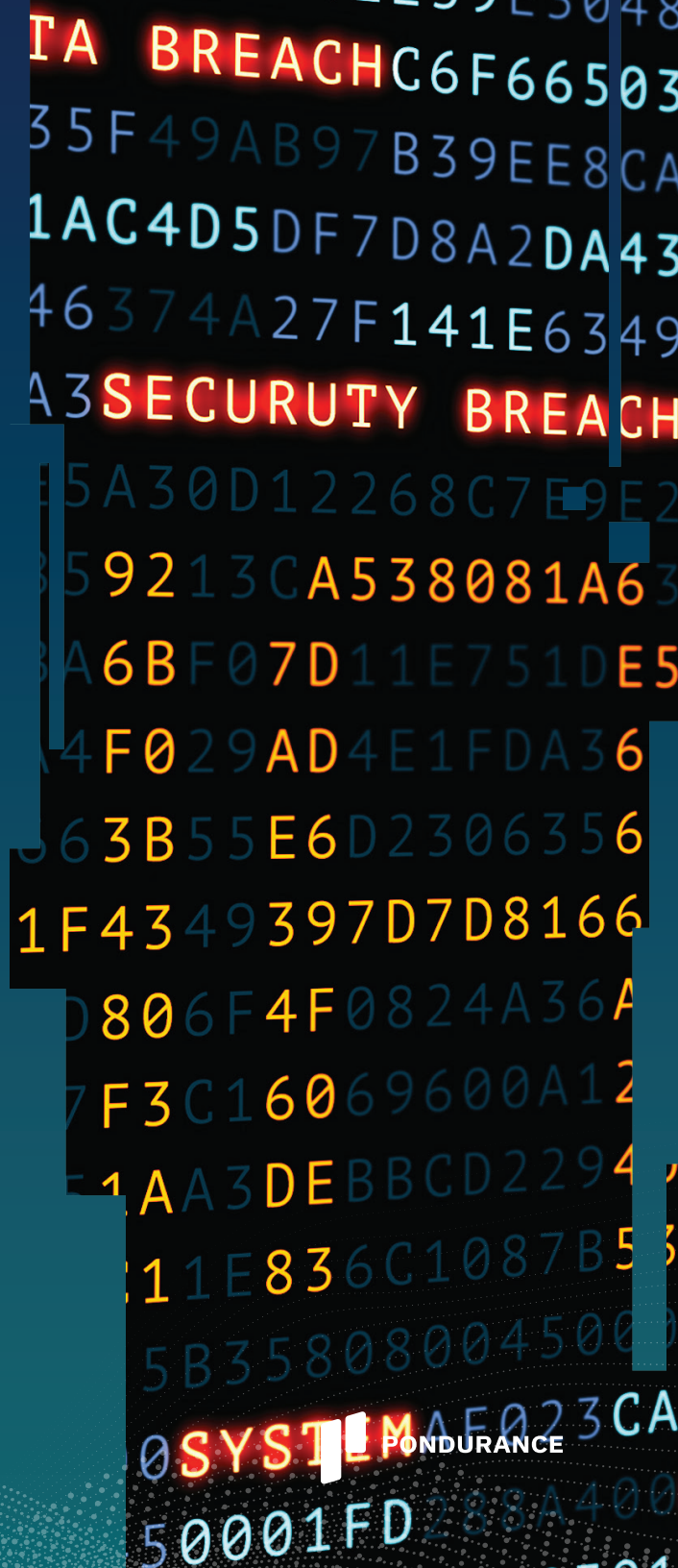
The scarcity of qualified cybersecurity resources is growing, which will compel the **NEED FOR TRADE-BASED CURRICULUMS AND CAREER OUTCOMES** (akin to plumbing, electrical, etc.).

# Conclusion

Cybercrime is not going away. If anything, the problem is getting worse, threatening to cripple organizations large and small. At the same time, security technology is evolving at a dizzying pace, such that newly acquired solutions are becoming legacy technology shortly after they're implemented. With both cyberthreats and cyber technology moving so fast, organizations should increasingly seek out the right partners to help manage and mitigate their risks — better protecting their business.

Dive further into our 2022 predictions in our webinar:
**What's Ahead? Cybersecurity Experts Share What to Expect in 2022**

WATCH HERE




PONDURANCE

# How Pondurance Can Help

Our mission is to ensure that every organization is able to detect and respond to cyberthreats — regardless of size, industry, or current in-house capabilities. We combine our advanced platform with decades of human intelligence to decrease risk to your mission.

## CLOSED-LOOP MANAGED DETECTION AND RESPONSE

Recognized by Gartner, Pondurance provides 24/7 U.S.-based SOC services powered by analysts, threat hunters, and incident responders who utilize our advanced cloud-native platform to provide you with continuous cyber-risk reduction. By integrating 360-degree visibility across log, endpoint, and network data and with proactive threat hunting, we reduce the time it takes to respond to emerging cyberthreats.

Pondurance MDR is the proactive security service backed by authentic human intelligence. Technology is not enough to stop cyberthreats. Human attackers must be confronted by human defenders.

## INCIDENT RESPONSE

When every minute counts, organizations need specialized cybersecurity experts to help them respond to a compromise, minimize losses, and prevent future incidents.

Pondurance delivers digital forensics and incident response services with an experienced team capable of guiding you and your organization every step of the way. This includes scoping and containing the incident, determining exposure through forensic analysis, and helping to quickly restore your normal operations.

## SECURITY CONSULTANCY SERVICES

Our specialized consultancy services will help you assess systems, controls, programs, and teams to uncover and manage vulnerabilities. Our suite of services ranges from penetration testing to red team exercises, along with compliance program assessments for highly regulated industries. We provide security incident response and business continuity planning to put you in the best position to defend against and respond to cyberattacks.



PONDURANCE

PONDURANCE

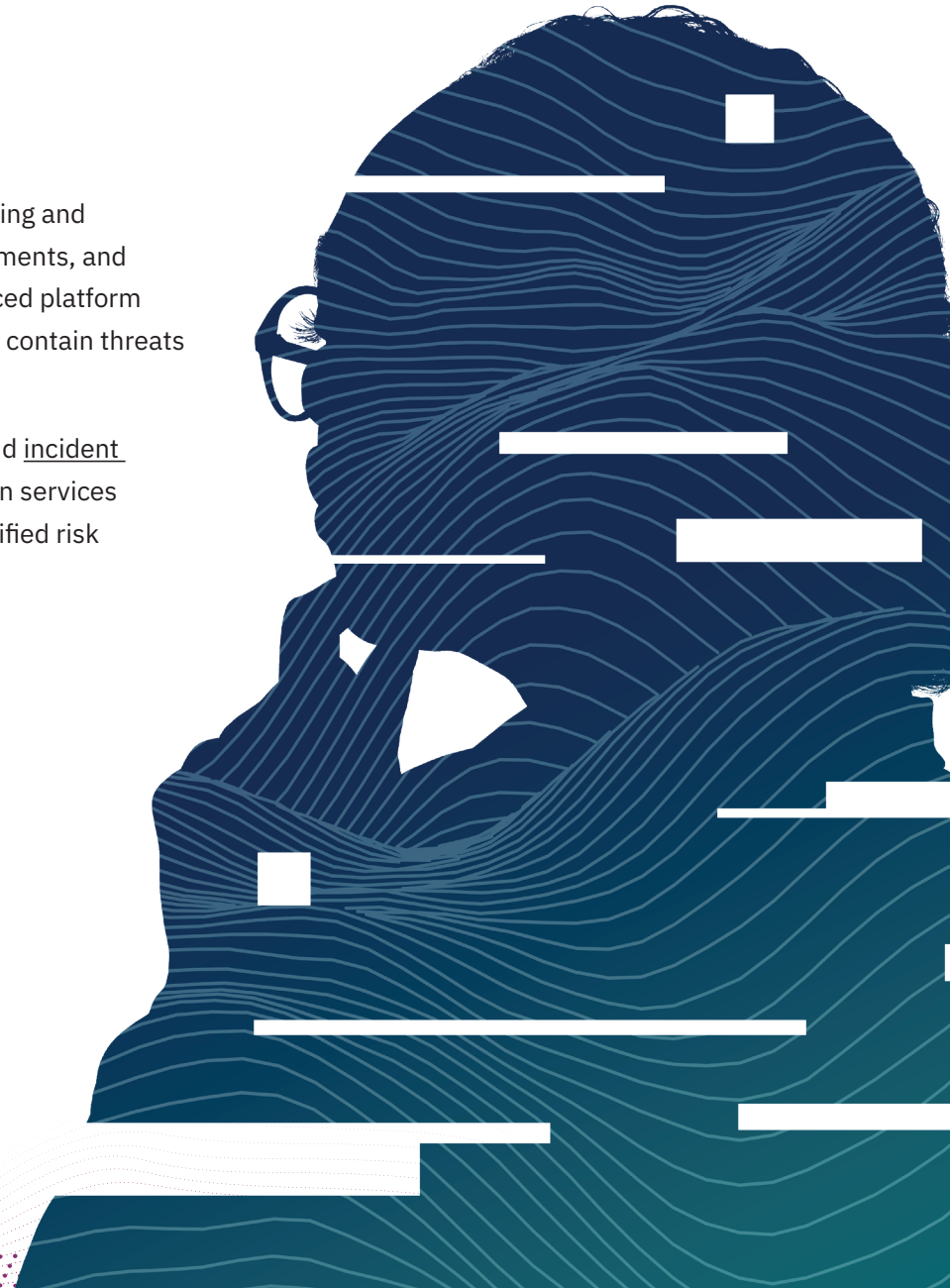
Copyright © 2021 Pondurance

# About Pondurance

**Pondurance delivers** world-class MDR services to industries facing today's most pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements, and digital transformation accelerated by a distributed workforce. By combining our advanced platform with our experienced team of analysts, we continuously hunt, investigate, validate, and contain threats so your own team can focus on what matters most.

Pondurance experts include seasoned security operations analysts, digital forensics and incident response professionals, and compliance and security strategists who provide always-on services to customers seeking broader visibility, faster response and containment, and more unified risk management for their organizations.

Visit **www.pondurance.com** for more information.



Sources:

1. **U.N. Official Warns Cybercrime Up 600% During COVID-19 Pandemic**, Newsy, May 23, 2020.

2. **Cybersecurity Professionals Stand Up to a Pandemic**, (ISC)², 2021.

**pondurance.com**

500 N. MERIDIAN ST., STE. 500
INDIANAPOLIS, IN 46204