SOFTPROM

www.softprom.com

WHITE PAPER

THE GLOBAL STATE OF INDUSTRIAL CYBERSECURITY 2021: RESILIENCE AMID DISRUPTION

CLAROTY

EXECUTIVE SUMMARY

This independent, global survey of 1,100 information technology (IT) and operational technology (OT) security professionals who work full time for enterprises that own, operate, or otherwise support components of critical infrastructure, explores how they have dealt with the significant challenges in 2021, their levels of resiliency, and priorities moving forward. Key findings include:

Ransomware is rampant and payments are prevalent

- A staggering 80% of respondents experienced an attack, with 47% reporting an impact to their OT/industrial control system (ICS) environment.
- More than 60% paid the ransom and just over half (52%) paid $500,000 USD or more.
- More than 90% disclosed the incident to shareholders and/or authorities and 69% believe timely reporting should be mandatory.

Digital transformation, remote work, and staffing shortages persist

- Digital transformation continues to accelerate since the pandemic, and remote/hybrid work will continue at 73% of organizations.
- Nearly 90% are looking to hire, but 54% say it is hard to find enough qualified OT security candidates.

Governance and executive oversight show strong leadership

- More than half of the respondents say their organization's C-suite and board are very involved in cybersecurity decision-making and oversight.
- More than 60% are centralizing OT and IT governance under the CISO – a recommended best practice. Gaps in processes and technology remain
- More than 65% rate their organization's vulnerability management strategy as moderately to highly proactive, yet ransomware attacks are highly successful.
- Nearly 30% are sharing passwords, 57% employ usernames and passwords, and 44% use VPNs – all areas of opportunity to strengthen resilience.

Investments and priorities aimed at building resilience

- More than 80% of respondents report that both their IT and OT/ICS security budgets have increased.
- Implementing new technology solutions is the top cybersecurity priority, with the Oil & Gas and IT Hardware sectors leading the way, and training is second.

INTRODUCTION

Industrial organizations dealt with significant challenges in 2021. Cyberattacks on the Oldsmar, Florida water facility, Colonial Pipeline, and JBS, as well as the SolarWinds supply chain attack, propelled industrial cybersecurity to the national and global stage. Millions of people have woken up to the staggering financial and societal repercussions when critical infrastructure is disrupted. On top of this, business leaders continue to deal with the impact of the COVID-19 pandemic while determining how to operate efficiently and securely. It is against this backdrop that organizations must strive to remain resilient despite unprecedented and unpredictable issues.

To understand how industrial organizations are navigating these uncharted waters, Claroty's 2021 survey focused on:

- The trifecta of disruptions they are facing – ransomware attacks, digital transformation, and remote work
- Key aspects to resiliency – governance, best practices, and investment
- Policies and priorities moving forward

METHODOLOGY

Claroty contracted with Pollfish to conduct a survey of information technology (IT) and operational technology (OT) security professionals in the United States (500), Europe (300), and Asia-Pacific (300). Only individuals who work full time in IT security, OT/industrial control system (ICS) security, or as an OT/ICS engineer or operator completed the survey, for a total of 1,100 respondents. Slightly more than half (55%) of the organizations included have at least $1B in revenue. More than a dozen industries are represented including IT Hardware, Oil & Gas (including Pipelines), Consumer Products, Electric Energy, Pharmaceutical/Life Sciences/Medical Devices, Transportation, Agriculture/Food & Beverage, Heavy Industry, Water & Waste, and Automotive. The survey was completed in September 2021.

KEY FINDINGS

A TRIFECTA OF DISRUPTIONS, WITH RANSOMWARE LEADING THE WAY

The rising tide of ransomware attacks targeting industrial organizations has reached new heights and no organization is immune. On a global basis, a staggering 80% of respondents experienced an attack, and 47% said it impacted the OT/ICS environment. More than 90% of organizations that were attacked disclosed the incident to shareholders and/or authorities, and reported the impact was substantial or significant in almost half (49%) of the cases.

Looking more closely at the distribution of attacks, in industries including IT Hardware, Oil & Gas, Water & Waste, and Automotive, 90% were impacted by ransomware and 87% in Heavy Industry and Electric Energy. Not surprisingly, the larger the organization, the more likely an attack, as that's where the money is; far fewer (63%) SMBs (<$500M annual revenue) report being impacted by ransomware.

Q1. Has your organization experienced a ransomware attack within the past year?

	GLOBAL	U.S.	APAC	EUROPE
Yes – impacted IT environment only	32.36%	36.40%	31.00%	27.00%
Yes – impacted OT/ICS environment only	20.27%	18.80%	20.00%	23.00%
Yes – impacted both IT and OT/ICS environments	27.09%	29.40%	27.00%	23.33%
No	16.09%	11.00%	20.67%	20.00%
I'm not sure	4.18%	4.40%	1.33%	6.67%

Q2. What was the scope of impact on operations?

	GLOBAL	U.S.	APAC	EUROPE
None or minimal – operations were never shutdown	14.60%	16.08%	13.68%	12.73%
Partial impact to a site or business function	36.03%	32.15%	39.74%	39.55%
Substantial impact to more than one site or function for less than a week	25.43%	24.11%	27.35%	25.91%
Substantial impact to more than one site or function for more than a week	16.19%	16.78%	14.53%	16.82%
Significant of full operations shut down for more than a week	7.75%	10.87%	4.7%	5.00%

Q3. Did your organization disclose the incident to shareholders and/or authorities?

	GLOBAL	U.S.	APAC	EUROPE
Both shareholders and authorities	59.18%	64.54%	58.55%	49.55%
Shareholders only	18.70%	13.95%	22.22%	24.09%
Authorities only	12.88%	12.06%	12.39%	15.00%
Neither shareholders nor authorities	5.02%	5.91%	2.99%	5.45%
I'm not sure	4.22%	3.55%	3.85%	5.91%

For organizations that experienced a ransomware attack, the financial impact was significant. On a global basis, more than 60% paid the ransom and, of those, just over half (52%) paid $500,000 USD or more. The U.S. led the way, where 76% paid the ransom and 57% paid $500,000 or more, versus 51% that paid in APAC and 49% in Europe. Payouts also trended lower in those regions, concentrated in the $100,000 - $500,000 range.

What's driving this decision to pay the ransom? As the adage goes, "time is money." Regardless of region, a majority of respondents estimated a loss in revenue per hour of downtime to their operations equal to or greater than the payout. So, the financial model seems to favor paying the ransom given this equation and what's at stake. This reasoning is also likely why on a global basis 69% of respondents believe it should be legal to pay ransoms. To change the financial calculus, what's required is a system of incentives and disincentives that favor better controls and risk governance up front.

Q4. Did your organization pay the ransom?

	GLOBAL	U.S.	APAC	EUROPE
Yes, we paid	62.14%	76.36%	50.85%	46.82%
No, we did not pay	31.70%	18.44%	44.02%	44.09%
I'm not sure	6.16%	5.20%	5.13%	9.09%

Q5. How much was the payment?

	GLOBAL	U.S.	APAC	EUROPE
Less than $100,000 USD	15.96%	15.79%	15.13%	17.48%
$100,000 - $500,00O USD	32.11%	26.93%	40.34%	38.83%
$500,000 - $1,000,000 USD	30.46%	29.72%	30.25%	33.01%
$1,000,000 - $5,000,000 USD	14.68%	17.65%	13.45%	6.80%
More than $5,000,000 USD	6.79%	9.91%	0.84%	3.88%

Q6. How much revenue would the operational impact of a downtime event cost your organization per hour?

	GLOBAL	U.S.	APAC	EUROPE
Less than $100,000 USD	20.64%	19.00%	24.00%	20.00%
$100,000 - $500,00O USD	28.09%	25.60%	29.67%	30.67%
$500,000 - $1,000,000 USD	22.27%	23.00%	21.67%	21.67%

$1,000,000 - $5,000,000 USD	14.45%	16.00%	14.33%	12.00%
More than $5,000,000 USD	8.73%	12.20%	4.67%	7.00%
I don't know	5.82%	4.20%	5.67%	8.67%

Q7. In your opinion, should it be legal or illegal to pay the ransom after being impacted by ransomware?

	GLOBAL	U.S.	APAC	EUROPE
Legal, and there should be no requirement to report to regulators or authorities	28.00%	36.60%	22.67%	19.00%
Legal, as long as the payment is reported to regulators or authorities	41.45%	40.80%	45.00%	39.00%
Illegal	21.09%	14.40%	25.33%	28.00%
I'm not sure	9.45%	8.20%	7.00%	14.00%

DIGITAL TRANSFORMATION AND REMOTE WORK CONTINUE

Respondents resoundingly report that digital transformation has accelerated since the start of the COVID-19 pandemic and, on a global basis, some level of remote work will continue at 73% of organizations for the foreseeable future. Digital transformation, the inherent increase in connectivity between IT and OT networks, and remote access for workers unlock tremendous business value. But these changes to OT/ICS environments also introduce risk by creating additional vectors for attackers. Results have played out in the headlines and spurred renewed warnings by the government on the risk of connecting industrial networks to IT networks and the need for a heightened state of awareness and controls.

Q8. Has the speed of your organization's digital transformation accelerated since the start of the COVID-19 pandemic?

	GLOBAL	U.S.	APAC	EUROPE
Yes, it has significantly accelerated	51.64%	58.20%	48.33%	44.00%
Yes, it has somewhat accelerated, but more could be done	38.55%	32.20%	49.33%	38.33%
No, it has not accelerated	9.82%	9.60%	2.33%	17.67%

Q9. What is your organization's current policy regarding onsite vs. remote work as it relates to the COVID-19 pandemic?

	GLOBAL	U.S.	APAC	EUROPE
100% onsite	21.64%	27.00%	17.67%	16.67%
100% remote	16.45%	15.20%	15.67%	19.33%
Only essential employees allowed/required to be onsite	29.55%	23.00%	39.00%	31.00%
Hybrid onsite/remote (mandated)	20.09%	21.40%	18.00%	20.00%
Hybrid onsite/remote (optional)	9.45%	10.20%	9.67%	8.00%
Other	2.82%	3.20%	0.00%	5.00%

Q10. Once the COVID-19 pandemic is over, how will your organization's remote work policy change, compared to what it was before the pandemic?

	GLOBAL	U.S.	APAC	EUROPE
100% onsite	27.00%	31.80%	26.00%	20.00%
100% remote	11.82%	13.60%	9.33%	11.33%
Only essential employees allowed/required to be onsite	21.82%	19.80%	26.00%	21.00%
Hybrid onsite/remote (mandated)	17.91%	15.40%	20.00%	20.00%
Hybrid onsite/remote (optional)	11.73%	9.20%	13.67%	14.00%
	7.27%	8.00%	5.00%	8.33%
Other	2.45%	2.20%	0.00%	5.33%

THE STATE OF RESILIENCY, STARTING WITH GOVERNANCE

This survey shows that organizations have internalized the lessons learned from high-profile cyberattacks and are prioritizing cybersecurity by increasing investments and implementing new or updated processes and controls. For example, on a global basis more than half of the respondents say their organization's C-suite and board are very involved in cybersecurity decision-making and oversight, which bodes well for ongoing investment and prioritization. Following recommended best practice, on a global basis more than 60% are centralizing OT and IT governance under the CISO. What's more, the majority (62%) are aligned with government direction towards mandatory, timely reporting of cybersecurity incidents affecting IT and OT/ICS systems.

Q11. Has your organization made any of the following changes since the high-profile ransomware incidents involving Colonial Pipeline and JBS that occurred earlier in 2021? (multiple answers permitted)

	GLOBAL	U.S.	APAC	EUROPE
Cybersecurity is a bigger priority now that it was before the incidents	53.91%	60.80%	52.33%	44.00%
We are increasing our investments in cybersecurity	54.00%	54.80%	55.00%	51.67%
We are implementing new and/or updated cybersecurity controls and processes	41.09%	48.80%	40.00%	29.33%
None of the above	5.09%	4.40%	2.33%	9.00%

Q12. Who is ultimately responsible for the cybersecurity of your organization's OT/ICS?

	GLOBAL	U.S.	APAC	EUROPE
CISO and/or security operations	60.82%	65.60%	64.33%	49.33%
COO and/or plant manager	25.55%	22.40%	28.67%	27.67%
I'm not sure	8.64%	6.40%	6.67%	14.33%
Other	5.00%	5.60%	0.33%	8.67%

Q13. To what degree is the head of your organization's C-suite/executive team involved in cybersecurity-related decision making and oversight?

	GLOBAL	U.S.	APAC	EUROPE
Very involved	52.36%	62.20%	50.00%	38.33%
Involved on a limited basis	36.82%	26.20%	45.67%	45.67%
Not involved at all	6.55%	6.40%	3.67%	9.67%
I'm not sure	4.27%	5.20%	0.67%	6.33%

Q14. Is your organization's board of directors involved in cybersecurity-related decision making and oversight?

	GLOBAL	U.S.	APAC	EUROPE
Very involved	50.27%	59.00%	44.67%	41.33%
Involved on a limited basis	37.55%	27.80%	48.33%	43.00%

Not involved at all	8.36%	8.40%	5.33%	11.33%
I'm not sure	3.82%	4.80%	1.67%	4.33%

Q15. In your opinion should the timely reporting of cybersecurity incidents affecting IT and OT/ICS systems within your organization to government regulators be mandatory or voluntary?

	GLOBAL	U.S.	APAC	EUROPE
Mandatory	62.73%	68.00%	62.00%	54.67%
Voluntary	28.55%	24.80%	31.33%	32.00%
Undecided	8.73%	7.20%	6.67%	13.33%

On a global basis, confidence in the capabilities of their IT security professionals to manage the OT/ICS environment's cybersecurity continues to grow, reaching 65% up from 61% in our previous survey conducted last year. But there is an ever-increasing need for security professionals. Nearly 90% are looking to hire, with 40% saying the need is urgent and 54% reporting it has been somewhat difficult to find enough candidates with the skills and experience required to properly manage an OT network's cybersecurity.

Q16. Do the IT security professionals in your organization have the skills and experience required to properly manage your OT/ICS environment's cybersecurity?

	GLOBAL	U.S.	APAC	EUROPE
Yes	65.82%	70.80%	67.67%	55.67%
Somewhat	29.27%	23.60%	31.33%	36.67%
No	4.91%	5.60%	1.00%	7.67%

Q17. Is your organization actively looking to hire more industrial cybersecurity professionals?

	GLOBAL	U.S.	APAC	EUROPE
Yes we are, urgently	39.91%	49.80%	29.67%	33.67%
Yes we are, in the long term	49.91%	41.00%	62.00%	52.67%
No, we are not	10.18%	9.20%	8.33%	13.67%

Q18. Has it been difficult to find enough candidates that have the skills and experience required to properly manage an OT network's cybersecurity?

	GLOBAL	U.S.	APAC	EUROPE
Yes, it has been extremely difficult	34.21%	44.05%	26.91%	24.71%
Yes, it has been somewhat difficult	54.15%	44.71%	64.36%	59.85%
No, it has not been difficult	11.64%	11.23%	8.73%	15.44%

BEST PRACTICES – PROCESSES AND TECHNOLOGY

Most respondents categorize their organization's cybersecurity maturity at level 4, the managed level, with Europe the exception at maturity level 3. And on a global basis more than 65% rate their vulnerability management strategy as moderately to highly proactive, with Europe at 55%. Yet ransomware attacks are still highly successful.

Q19. How would you rate your organization's cybersecurity maturity, based on the capability maturity matrix (CMM)*?

	GLOBAL	U.S.	APAC	EUROPE
CMM 1: Initial level	7.18%	10.20%	5.00%	4.33%
CMM 2: Repeatable level	15.73%	15.20%	16.67%	15.67%
CMM 3: Defined level	24.82%	18.40%	28.33%	32.00%
CMM 4: Managed level	31.27%	29.60%	36.33%	29.00%
CMM 5: Optimizing level	16.18%	21.40%	10.33%	13.33%
I'm not sure	4.82%	5.20%	3.33%	5.67%

**Note: Developed by the Software Engineering Institute of Carnegie Mellon University, the CMM is a long-established framework for continuous process improvement that breaks the five maturity levels into evolutionary steps. The objective is to improve the quality of the development and delivery of products and services, in this case cybersecurity.*

Q20. Which of these best describes your vulnerability management strategy?

	GLOBAL	U.S.	APAC	EUROPE
Highly Proactive – We conduct vulnerability assessments continuously	30.27%	42.80%	21.33%	18.33%
Moderately Proactive – We conduct vulnerability assessments frequently	35.73%	30.60%	43.33%	36.67%
Mildly Proactive – We conduct vulnerability assessments occasionally	17.18%	12.20%	21.33%	21.33%
Reactive – We have a dedicated team/process for assessing vulnerabilities when brought to our attention by a third party	9.36%	6.80%	11.00%	12.00%
None – We do not have an established process for assessing vulnerabilities	2.82%	2.40%	1.67%	4.67%
I don't know	2.64%	2.40%	1.33%	4.33%
Other	2.00%	2.80%	0.00%	2.67%

Improved cyber training is needed to help thwart ransomware attacks. On a global basis, a third (33%) of respondents say that training related to preventing and managing future cyberattacks is not adequate or not provided. In our 2020 survey, 83% reported training related to working remotely was provided. However, it appears skills development to mitigate risk from attacks that take advantage of vulnerabilities spurred by this new, distributed environment is lacking. As the answers below reveal, OT remote access needs improvement. Nearly 30% are sharing passwords (although this is closer to 20% in APAC and Europe), 57% employ usernames and passwords, and 44% use VPNs. Basic cyber hygiene, stronger passwords, and secure remote access solutions can help strengthen resilience against attacks.

Q21. To what extent does your organization provide training or encourage the development of new skills related to preventing and managing future cyberattacks (such as ransomware)?

	GLOBAL	U.S.	APAC	EUROPE
Not at all	6.82%	7.20%	3.00%	10.00%
To a limited extent but not adequate	26.55%	21.80%	30.67%	30.33%
To an adequate extent based on our risk tolerance	39.91%	37.60%	44.67%	39.00%
We have a risk aware culture that encourages cyber risk management training and skill development	26.73%	33.40%	21.67%	20.67%

Q22. Which of the following has your organization implemented for OT remote access? (multiple answers permitted)

	GLOBAL	U.S.	APAC	EUROPE
VPN	44.09%	42.60%	50.00%	40.67%
Username and password	56.73%	59.00%	61.67%	48.00%
Shared passwords	29.09%	39.20%	21.67%	19.67%
Single-factor authentication	35.91%	42.80%	33.67%	26.67%
Remote user monitoring	37.55%	40.80%	37.33%	32.33%
Multi-factor authentication	46.64%	48.40%	49.00%	41.33%
Nothing	7.73%	9.80%	3.33%	8.67%
Other	4.91%	6.00%	0.00%	8.00%

INVESTMENTS AND PRIORITIES

More than 80% of respondents report that both their IT and OT/ICS security budgets have increased since the start of the COVID-19 pandemic. The number is close to 90% in industries including IT Hardware, Oil & Gas, and Electric Energy. This widespread increase in investment is likely a direct result of executive- and board-level prioritization of cybersecurity amidst the scourge of ransomware that has disrupted operations for most industrial organizations surveyed, as well as the high-profile SolarWinds compromise which put IT companies on notice that they could be launching pads for this particularly insidious type of attack.

Q23. How has your organization's IT security budget changed since the start of the COVID-19 pandemic?

	GLOBAL	U.S.	APAC	EUROPE
IT security budget has significantly increased	39.73%	50.40%	35.00%	26.67%
IT security budget has moderately increased	43.45%	34.00%	55.33%	47.33%
IT security budget has decreased	9.27%	8.60%	5.67%	14.00%
IT security budget has not changed	7.55%	7.00%	4.00%	12.00%

Q24. How has your organization's OT/ICS security budget changed since the start of the COVID-19 pandemic?

	GLOBAL	U.S.	APAC	EUROPE
OT/ICS security budget has significantly increased	36.27%	49.80%	28.00%	22.00%
OT/ICS security budget has moderately increased	45.55%	33.80%	62.00%	48.67%
OT/ICS security budget has decreased	9.18%	9.40%	5.33%	12.67%
OT/ICS security budget has not changed	9.00%	7.00%	4.67%	16.67%

RECOMMENDATIONS

Consistent with results from our previous survey, respondents across regions consistently and overwhelmingly rank implementing new technology solutions as the top priority, with respondents in Oil & Gas and IT Hardware tilting the ranking at 57% and 49% respectively. That said, Europe lists training as a close second and SMBs prioritize training and technology equally at the top.

Q25. What would you like to see be your organization's highest cybersecurity priority moving forward?

	GLOBAL	U.S.	APAC	EUROPE
Implement new technology solutions	40.27%	46.60%	38.67%	31.33%
Hire more staff	16.09%	14.80%	14.00%	20.33%
Provide training for existing staff	23.82%	18.60%	29.00%	27.33%
Enabling a long-term/indefinitely remote workforce	10.73%	8.60%	14.67%	10.33%
Increase overall budget	7.45%	9.60%	3.67%	7.67%
Other	1.64%	1.80%	0.00%	3.00%

As this survey has shown, industrial organizations are on the right track. A majority of organizations have already extended existing IT risk management and governance processes to include OT networks, with responsibility under the CISO, and have increased both IT and OT/ICS security budgets. However, the success ransomware attacks have had on most of these organizations, and the continuation of digital transformation and remote work, are undeniable. Organizations must remain alert and continue to build resilience.

The industrial cybersecurity industry has made tremendous progress in creating technology solutions that help eliminate blind spots and close security gaps to build resilience. Furthermore, solutions that can be implemented without burdening existing infrastructure and personnel with unnecessary traffic, hardware, complex configurations, lengthy deployments, or steep learning curves are crucial given the hiring challenges nearly every organization is facing.

The following five recommended technologies and processes can help security leaders and their teams better protect their OT environments and enable the business in today's hyperconnected world.

1. **Extend risk governance to include cyber-physical assets.** Devices that are not designed with security in mind introduce risk when connected to IT and OT networks. This includes all Industrial IoT, ICS, and Enterprise IoT components. Extending governance to include these assets is a challenging step for many organizations since it's not an easy task to even identify them. It's a process that might take iterations. Thankfully, in the last few years the industry has made tremendous progress in technology that makes it easier to discover such assets and profile their exposure, risk, and vulnerabilities.

2. **Maintain proper segmentation.** There are many business processes and applications that need to communicate across the IT/OT boundary, so organizations need to ensure this is done in a secure way. Ensuring an organization's OT network and assets are isolated from IT in a manner that aligns with segmentation best practices can be a highly effective means of stopping the lateral spread of ransomware and other malware from IT to OT. In addition to segmentation between IT and OT networks, deploy virtual segmentation to zones within the OT environment. This will help detect lateral movement within the OT networks. And when remote operations need access directly into the OT networks, make sure this is done through a secure remote access connection with strict controls over users, devices, and sessions. These solutions can be deployed without burdening the OT environment.

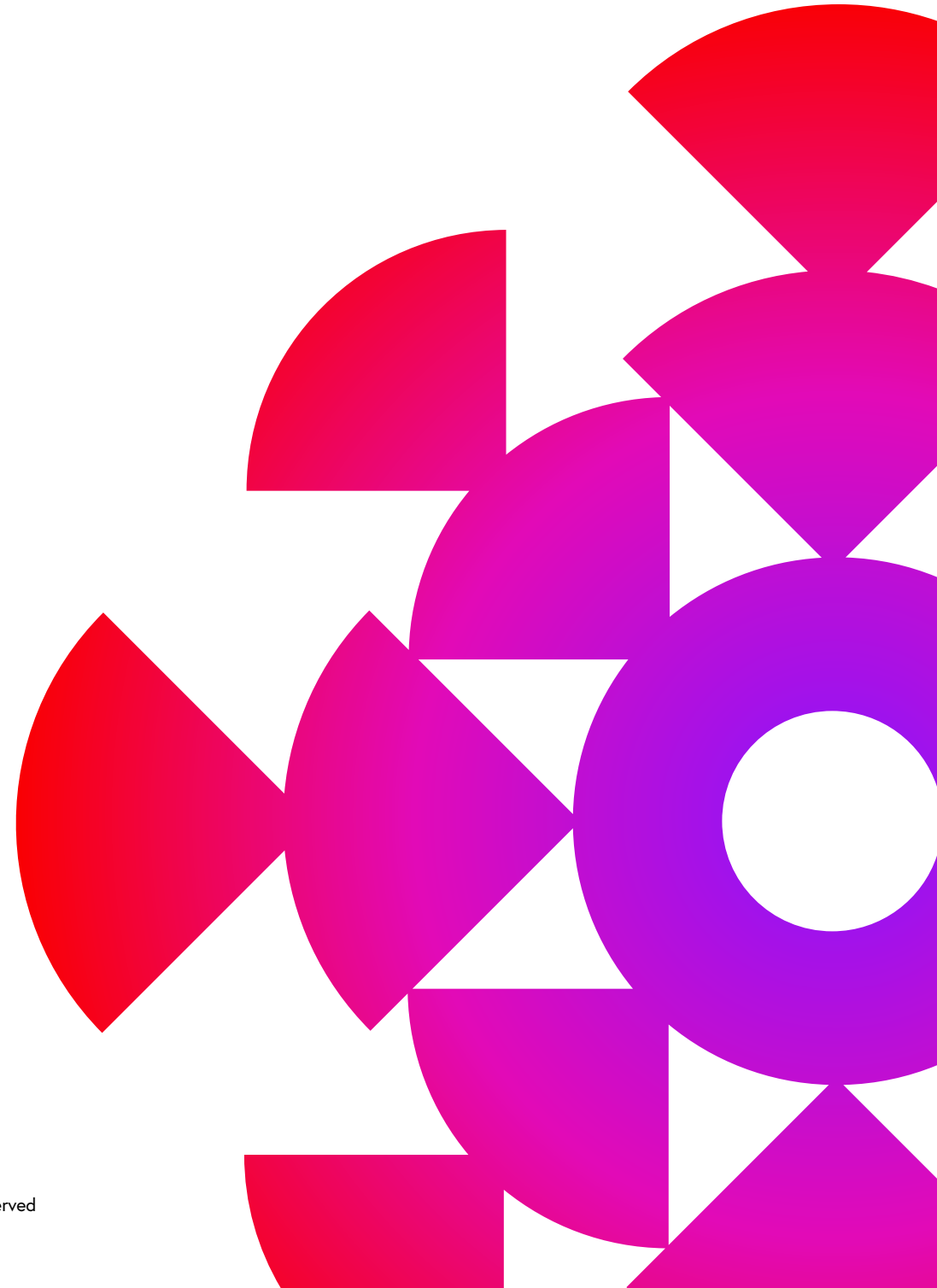
3. **Practice good cyber hygiene.** Ensure that cyber hygiene extends to OT and IoT devices. This includes the use of strong passwords (and not sharing passwords amongst different users), a password vault, and multi-factor authentication. Some processes, like patching legacy systems, might be more challenging or not possible. If that is the case, identify and implement compensating controls such as firewall rules and access control lists. The Cybersecurity and Infrastructure Security Agency (CISA) has a number of no-cost hygiene tools – including scanning, assessments, and testing – to help reduce exposure to threats.

4. **Implement a robust system monitoring program.** Being able to monitor for threats in both IT and OT networks and anything that is traversing that boundary is imperative for effective and efficient detection and response. Agentless solutions that are purpose-built for continuous threat monitoring across the OT network, can be implemented quickly, integrate equally well with OT and IT systems and workflows, and allow IT and OT teams to look at OT environments together. Working from the same set of information these teams take specific steps to manage and mitigate risk from both known and unknown, emerging threats.

5. **Assess and build preparedness.** Implementing the above capabilities and strengthening resilience gives security leaders and teams peace of mind. Running tabletop exercises of ransomware attacks provides a deeper understanding of organizational and technical preparedness. This affords organizations an opportunity to create an improved incident response plan that will build confidence in preparedness and in-the-moment decision making, and resilience to such attacks. If not already in place, formalize partnerships with incident response and legal firms. When these firms already have established working relationships with internal stakeholders and teams, have visibility into existing IT and OT infrastructure and controls, and understand the business and risk profile, they are capable of providing better counsel, faster in the face of an attack.

CONCLUSION

As digital transformation and remote work continued throughout 2021, ransomware attacks on IT and OT/ICS networks were rampant and payouts were significant. As long as the financial model continues to favor paying the ransom, these threats will continue. The only way to mitigate the risk is to understand how to make hyperconnectivity more secure. Gaps in processes and technology, some that have existed for years, must be addressed. Fortunately, organizations across the globe have strong executive leadership and trusted cybersecurity experts at the helm. Standing together, they are on the right track. Extending governance to include OT networks, allocating additional resources, and prioritizing best practices and controls, they are building resilience amid disruption.



SOFTPROM

CLAROTY