accenture

Ransomware response and recovery

How to be more resilient in the face of ransomware threats

Why ransomware?

According to Christopher Krebs, former Director of the Cybersecurity and Infrastructure Security Agency (CISA), "You've got to start with what really matters the most and then you work out from there. So, from that perspective, ransomware is the biggest threat." [1]

Impacts vary, but, in many cases, ransomware disrupts businesses for significant periods—or even forces them to suspend operations or close.

A growing population of highly capable cyber extortionists is developing a new means to counter defenses and increase the level of disruption they can inflict, constantly. Threats are widespread; they extend across industry and the public/private sector, affecting large and small businesses alike.

Security leaders must understand and counter new ransomware challenges, strengthen defenses across people, processes, and technology and demonstrate why security is critical to the business strategy.

In short, security leaders need to help their organizations gain ransomware resilience—fast.

Today's top three challenges

#1 **Successful ransomware extortionists are ramping up attacks**

#2 **Ransomware operators are constantly improving their ability to disrupt**

#3 **Business growth and service strategies lack resilience**

What does ransomware look like?

Ransomware can create a crisis of systemic business risk and consumer trust

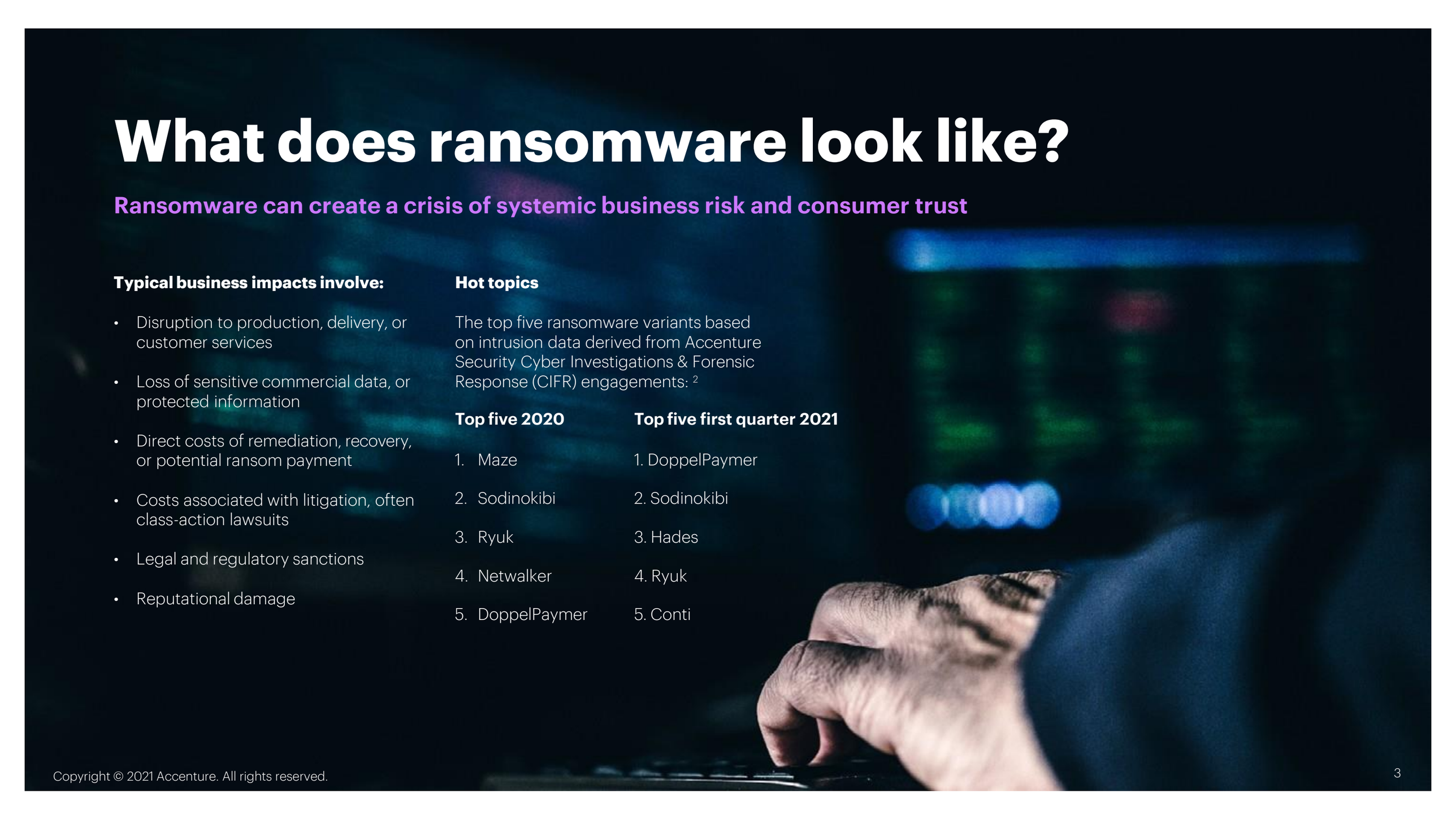
Typical business impacts involve:

- Disruption to production, delivery, or customer services
- Loss of sensitive commercial data, or protected information
- Direct costs of remediation, recovery, or potential ransom payment
- Costs associated with litigation, often class-action lawsuits
- Legal and regulatory sanctions
- Reputational damage

Hot topics

The top five ransomware variants based on intrusion data derived from Accenture Security Cyber Investigations & Forensic Response (CIFR) engagements: [2]

Top five 2020	Top five first quarter 2021
1. Maze	1. DoppelPaymer
2. Sodinokibi	2. Sodinokibi
3. Ryuk	3. Hades
4. Netwalker	4. Ryuk
5. DoppelPaymer	5. Conti



Challenge #1

Successful ransomware extortionists are ramping up attacks

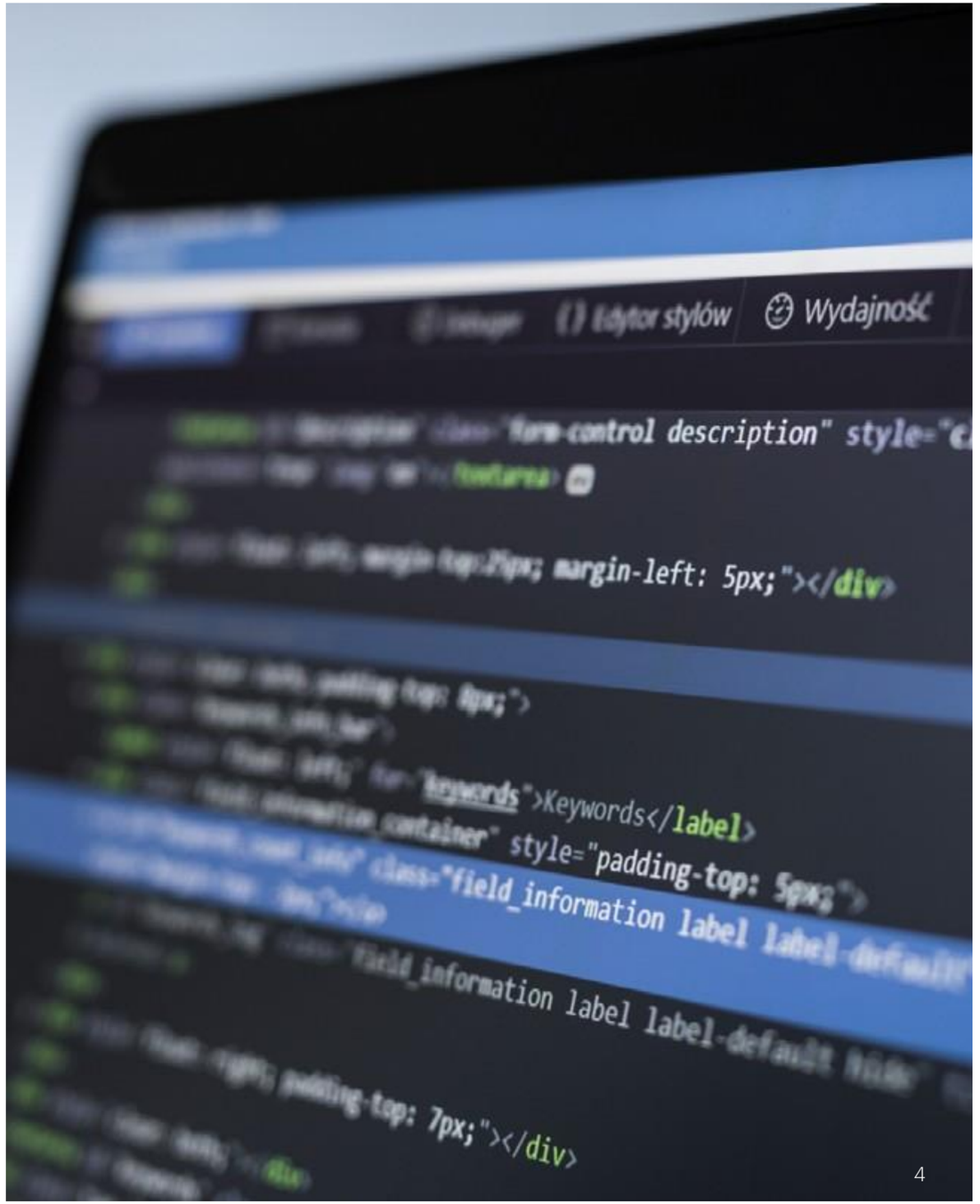
Established ransomware operators are upping their game as they continue to focus on new monetization opportunities and see no limits to the potential profits.

At the same time, the barrier to entry is low; ransomware tools and supporting operations are readily available through various markets and affiliate networks.

Alongside the opportunities presented by the pandemic, the population of extortionists is growing as new cybercriminals are drawn to the low-risk, high-reward operations.

To plan for resilience, organizations should focus on the business and operational risks presented by the threat across their unique value chain—and prioritize planning and defense efforts accordingly.

The Accenture CIFR team observed a 160% year-on-year increase in ransomware events in 2020—with little signs of any slowdown in early 2021.[3]



Challenge #2

Ransomware operators are constantly improving their ability to disrupt

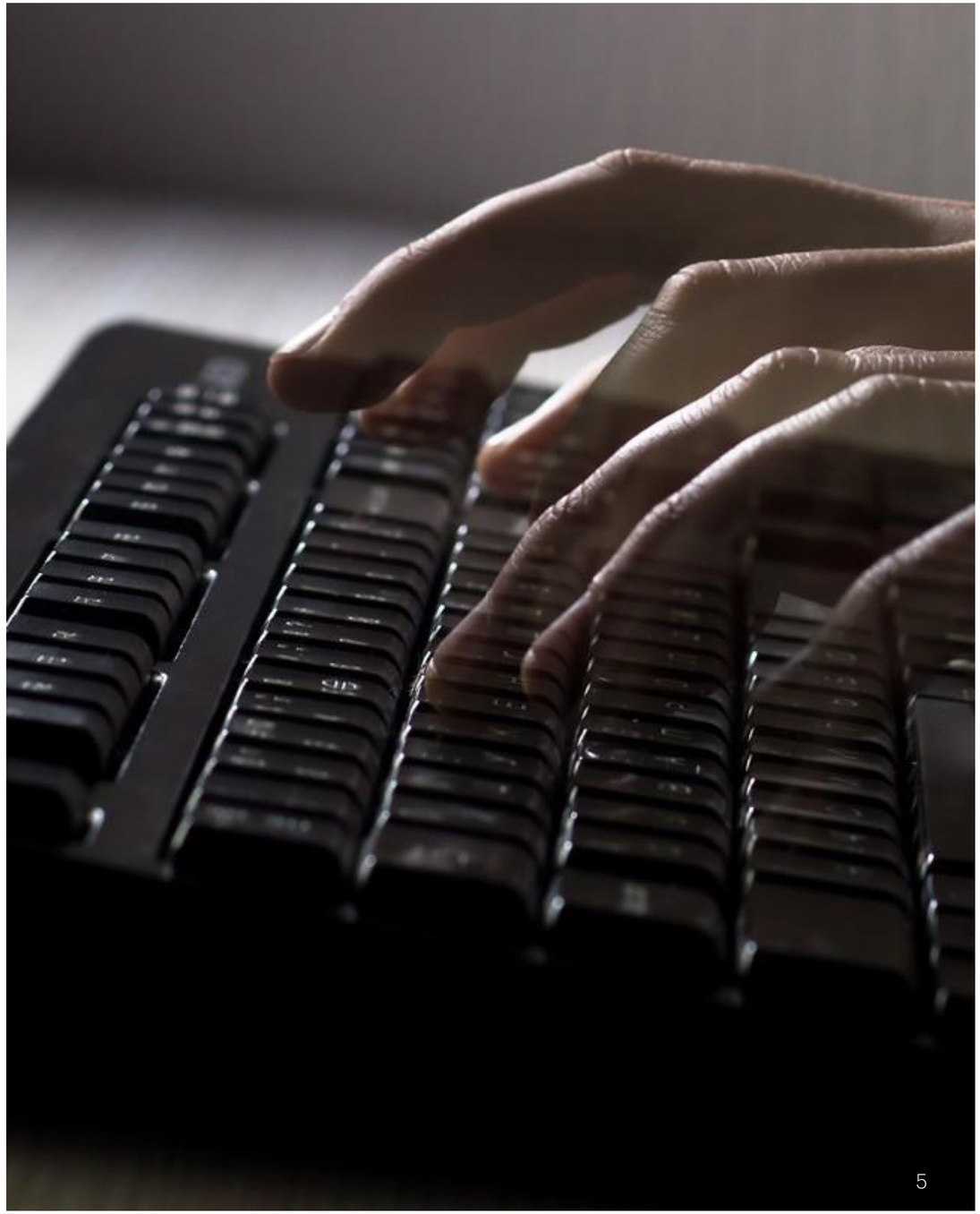
Cyber extortionists are incentivized to develop ever-more disruptive ways of working. The more disruption they can inflict, the larger the ransom they can demand.

Operators keep innovating, first using ransomware in a targeted way, against key assets, then combining that with data leak extortion. Now, there are indications that certain operators are increasing their ability to interfere with operational technology (OT) processes and refining other means to pressure payment, including layering distributed denial-of-service attacks with encryption and data leakage.

Commodification of the skills and services required—ranging from initial access brokers and intrusion specialists to ransomware-as-a-service models with partners and affiliates and specialist negotiator middle-men—is enabling and rewarding the development of new, more disruptive techniques.

In December 2020, extortionists targeted one of the world's largest manufacturers, claimed encryption of 1,200 servers, realized the theft of 100GB of data, deleted 20 to 30TB of backups and demanded a $34M ransom.[4]

One variant has stepped up its confrontational approach, delivering its ransomware notes through a retailer's receipt printer.



Challenge #3

Business growth and service strategies lack resilience

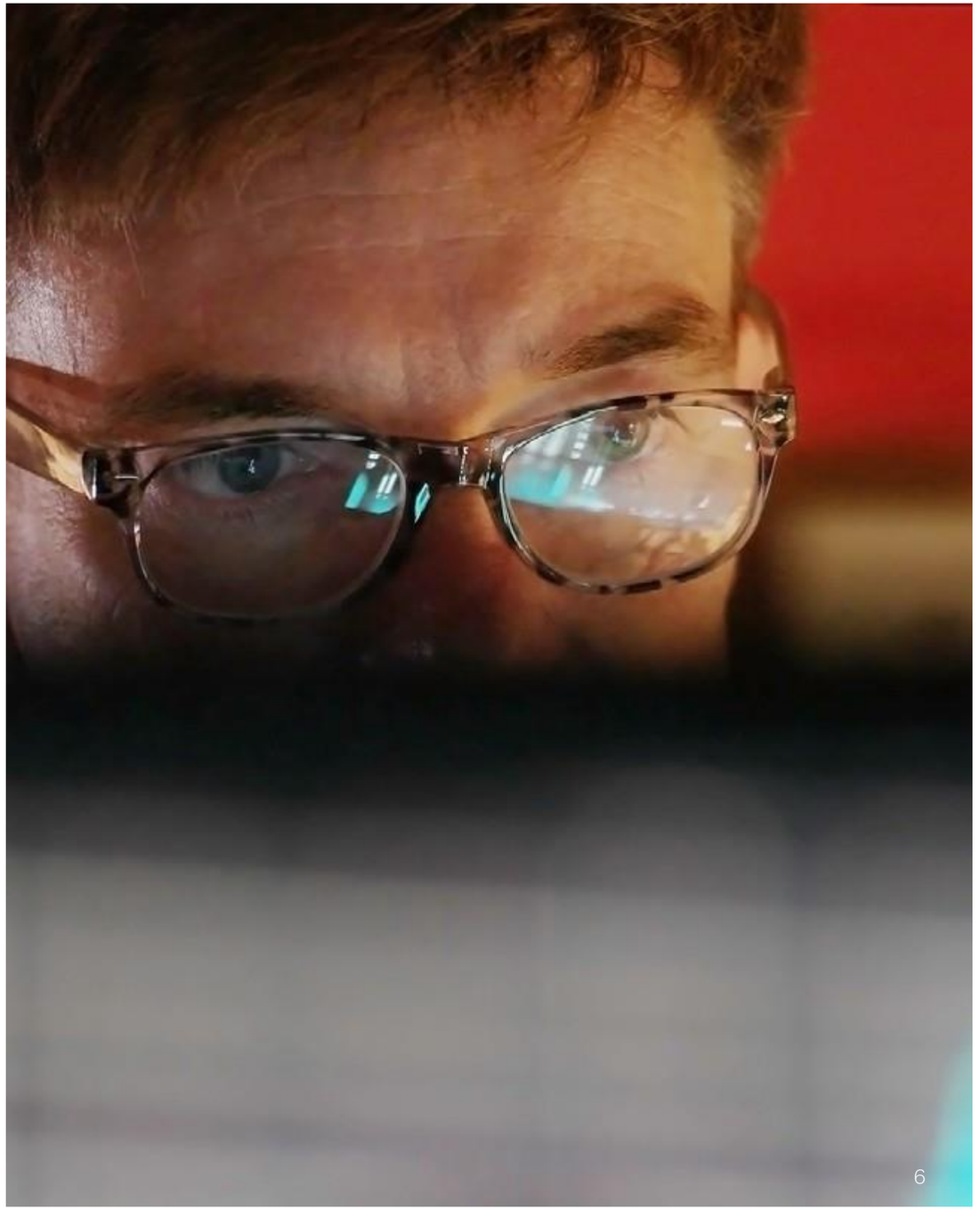
Downtime from ransomware is still growing. According to Coveware, firms experienced on average 23 days of downtime in the first quarter of 2021, up from 21 days in the fourth quarter of 2020. Downtime ranged from standstill to minor non-availability.[5]

Encryption can deny access and interrupt basic and vital resources, including internal and customer communications and platforms, as well as operational or production systems. Long periods of downtime can affect tens of millions of people. The theft and publication of data give attackers new extortion opportunities—such as the risk of regulatory sanctions if protected information is made available online.

Ransom demands are growing and becoming more customized—with threat actors assessing who is more likely to pay. If ransoms are paid, it can open the door to further criminality. Also, some ransomware operators have been sanctioned, potentially placing a ransom-paying victim in further legal jeopardy.

The Accenture CIFR team observed ransom demands ranging from US$100,000 to US$50M in 2020.[6]

In August 2020, a leading foreign exchange firm went into administration to lose more than 1,300 jobs. Administrators stated that a ransomware attack had caused a month of disruption and at times staff could not use computers to keep track of currency trading. The breach also disrupted online travel money services for leading global clients.[7]



Ransomware is evolving

Established operators extend reach and profits with new collaborations

A ransomware-as-a-service model has been transformative for extortionists. Owners of highly effective and widely disseminated malware strains, formerly known as "banking trojans," are working with intrusion specialists to infect and extort the maximum number of victims.

Ransomware operators often move fast

Often, operators have exfiltrated sensitive data and encrypted key assets within hours of an initial infection. Also, some companies are more commonly finding themselves targeted twice in quick succession by different actors.

New variants and enhanced tactics challenge defenses

Threats are going beyond IT to new technologies and platforms—there are at least seven known variants with features designed to target common industrial environment processes. Criminals have the resources to re-invest and innovate, regularly designing new, more effective tools and techniques to increase their operations' efficacy.

Organizations feel the pressure of payment strategies and regulatory demands

Aggressive operators are phoning victims directly, sometimes combining denial-of-service attacks with encryption and publication tactics. The United States federal government has released an advisory[8] reminding CISOs that by financing terrorism or financing banned organizations in the payment of a ransom, they are committing an offense. While in Europe, GDPR requires any potential breach to be reported to the regulator within 72 hours—or face sanctions.

What can you do now?

Operate under the assumption that you are already breached and focus on resilience across the end-to-end value chain

Focus on the basics

Keep security hygiene up to standard; maintain controls and continue patching; ensure visibility into and protection of crown jewel data.

Implement a holistic backup and recovery strategy with situational awareness of the current threat landscape.

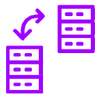
Ensure you have a crisis management and incident response plan that's in line with the current pandemic-driven operating environment.

Prevent and protect

Increase confidence through continuous validation and testing of your defenses.

Train and test employees frequently.

Ensure adequate visibility and coverage across the attack surface—use tooling, controls and telemetry to enhance your defense posture across layered prevention, detection, and agile response.



Know your operations

Model the threat against your operations and end-to-end value chain.

Understand how to backup and restore critical data at speed and scale across the business—strive for continuity of operations.

Be clear on policies and procedures—the response playbook is often the first thing regulators and litigants ask for after a breach.

Make it personal

CISOs cannot go it alone. Collaborate and prepare with Legal, Communications, senior management and external service providers, so everyone knows how to work together during an event.

Conduct crisis management and table-top exercises to test relationships.

Meet regularly with authorities, incident response partners and outside legal counsel to bolster support.

Prepare, prepare and prepare again

Threats are agile and you should be, too. Businesses don't evaluate their profit and loss or liquidity levels once a year—security should be no different.

Use planning and validation as an opportunity to constantly measure and improve resilience or adjust your course over time.

Pressure-test for when things go wrong.

So, you've been hit—what's next?

"Never let a good crisis go to waste"[9]—after any ransomware attack, CISOs should reflect on improvements to ease the impact of future events

1
Trace the attack

Use incident response, forensic analysis and threat intelligence to identify how the attack occurred and build a comprehensive understanding of the intrusion and measured impact. This is critical during and after the incident to inform defense posturing, comprehensive take-back planning in a domain compromise and safe recovery of business operations.

2
Collaborate and report

Work with legal counsel to ensure statutory obligations are fulfilled by reporting an incident to the appropriate authorities. Collaborate with industry partners, consortiums and law enforcement for greater threat awareness.

3
Learn from the experience

Quantify the financial and reputational impacts and identify metrics and resources to meet the C-suite's expectations for cyber resilience going forward. Talk to the C-suite so that business leaders can prioritize and oversee the measurement of cyber resilience, secure funding for improvements and incorporate it into business resilience plans.

4
Update risk mitigation plans

Evaluate current inherent and residual risk measurements and work with the business to identify any beyond acceptable levels. Apply an appropriate risk mitigation strategy that includes aspects such as controls deployment or security transfer mechanisms.

5
Strengthen defense posture

Get tactical: remediate identified vulnerabilities, update operating systems, deploy compensating controls, refine weak processes, harden the environment (across network, endpoint, and identity), improve cyber hygiene, enhance the efficacy of threat detection and response operations, address weaknesses in recovery processes and drive the necessary behavioral changes required to strengthen cybersecurity defenses.

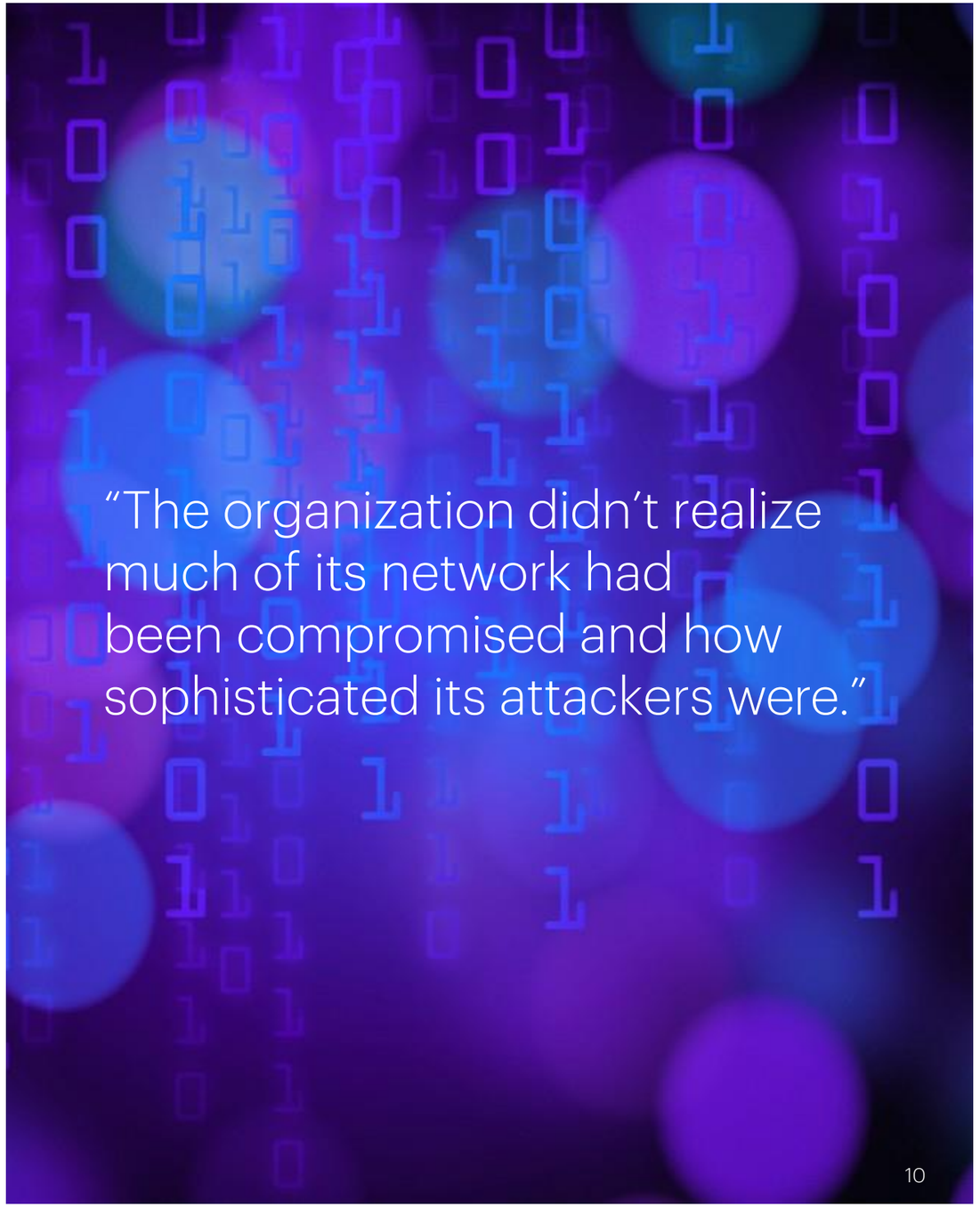
Who’s doing what?

An organization paid ransom twice following a failure of its antivirus protection measures. Once attackers had gained entry to its systems, they set about changing existing client security measures and controls to guarantee continued access. The organization didn’t realize how much of its network had been compromised and how sophisticated its attackers were.

A medium-sized manufacturer was preparing to replace all its virus detection software. It was unaware that attackers had infiltrated its network months prior and it was monitoring the company e-mail Web portal through a poorly protected administrative account. When the attackers discovered a planned upgrade, hackers launched an attack the weekend before countermeasures were planned to be deployed.

A Norwegian aluminum manufacturer was forced to halt some production and switch other units to manual operations after hackers blocked its systems. Its post-response analysis showed that attackers had been present in the network for three months when somebody clicked on the wrong e-mail. The forced shutdown cost the company US$52M.

An oil and gas company with a good recovery plan, validated backups, and a strong leadership team determined not to pay a ransom. When it was hit, it could get back up and running in less than one week. On the other hand, for a manufacturing customer who had not been validating its backups and had a piecemeal recovery process, it took six weeks to recover from an attack.



Ransomware incident response trends

A look back at 2020 intrusion data[10]

- Top industries impacted: Products[11] (38%) Resources[12] (33%), Healthcare and State and Local Government (17%)
- Initial ransom demands ranging from US$100K to US$50M
- Average operational downtime around 12 days
- Data extortion was incorporated in >60% of intrusions
- Dwell times range from 2.5 hours to around six months[13]
- Primary attack vectors: 1. Phishing, 2. Remote access, 3. Software vulnerability

Are you ready?

Being resilient means robust processes, training and coordination across the business value chain
Ask yourself:

What

- What are the most critical systems and data in your operations?
- What plans do you have in place? (such as business continuity, disaster recovery)
- What is your media strategy in the event of a crisis?

How

- How often do you pressure-test and exercise your plans?
- How quickly could you respond to and recover from a ransomware threat?
- How would you handle a full domain compromise?

Who

- Who are your decision-makers during a crisis?
- Who is responsible for negotiating or reviewing your extortion policy?
- Who handles incident response?

Contacts

Mark Raeburn
Managing Director
Cyber Defense
Accenture Security

Jacky Fox
Managing Director
United Kingdom & Ireland
Accenture Security

Ryan Leininger
Senior Manager
Cyber Defense
Accenture Security

References

1. Former US cyber chief calls for military to attack hackers, *Financial Times*, 2021, https://www.ft.com/content/27c09769-ceb5-46dd-824f-40b684d681ae
2. Looking back to see the future: CIFR DeLorean—2021 edition, Accenture, 2021, https://www.accenture.com/us-en/blogs/cyber-defense/cifr-delorean-2021-edition
3. Ibid
4. Foxconn electronics giant hit by ransomware, $34 million ransom, Bleeping Computer, 2020, https://www.bleepingcomputer.com/news/security/foxconn-electronics-giant-hit-by-ransomware-34-million-ransom/
5. Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound, Coveware, 2021, https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
6. Looking back to see the future: CIFR DeLorean—2021 edition, Accenture, 2021, https://www.accenture.com/us-en/blogs/cyber-defense/cifr-delorean-2021-edition
7. Travelex falls into administration, with loss of 1,300 jobs, *The Guardian*, 2020, https://www.theguardian.com/business/2020/aug/06/travelex-falls-into-administration-shedding-1300-jobs
8. Department of the Treasury, 2020, https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
9. Attributed to Sir Winston Churchill
10. CIFR observations
11. Products industries include: Automotive, Airline, Consumer Goods & Services, Hotels, Industrial Equipment, Life Sciences, Retail
12. Resources industries include: Energy (Oil & Gas), Chemicals, Metals/Mining, Utilities
13. Dwell time is the amount of time the threat actor is active in the victim organization's network—from first evidence of compromise through detection (or impact)

Appendix

Top ransomware variants observed by Accenture Security's CIFR team:

- **Conti:** First observed by cybersecurity teams in May 2020, it involves double extortion that that puts information and reputation at risk. It not only encrypts files on the infected host but also spreads to encrypt files on different hosts, potentially compromising the entire network.
- **DoppelPaymer:** A newer variant associated with the well-established Dridex Gang, whose leader was sanctioned and linked to Russia's Federal Security Service (FSB) by the United States Justice Department in December 2019.
- **Hades:** A ransomware campaign that has been ongoing since at least December 2020, Hades ransom notes share portions with the one used by the REvil ransomware operators; there is no evidence to suggest the threat groups or operations have any overlap.
- **Maze:** Maze operations changed the game by being the first cartel to pioneer the double extortion approach. It reportedly shut down in Q4 2020 (see https://techcrunch.com/2020/11/02/maze-ransomware-group-shutting-down/)
- **Netwalker:** Made a name for itself with a string of healthcare compromises but was interrupted by law enforcement interdiction that occurred in January 2021. Its operations were recently disrupted by international law enforcement agencies (see https://www.zdnet.com/article/us-and-bulgarian-authorities-dirsupt-netwalker-ransomware-operation/)
- **Ryuk:** Known for being prolific and aggressive. It benefits from strong working links with the effective and widely disseminated downloader malware, TrickBot and Emotet and conducted multiple high-impact compromises against United States hospitals in late 2020.

For more, visit Looking back to see the future: CIFR DeLorean—2021 edition

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services—all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 537,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners, and communities.
Visit us at **www.accenture.com**

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us @AccentureSecure on Twitter or visit us at **www.accenture.com/security**