



When will the threat of a cyberattack be enough to spark real organizational resilience?

Recent ransomware attacks serve as another reminder of the impact cyberattacks can have on organizations, governments and society

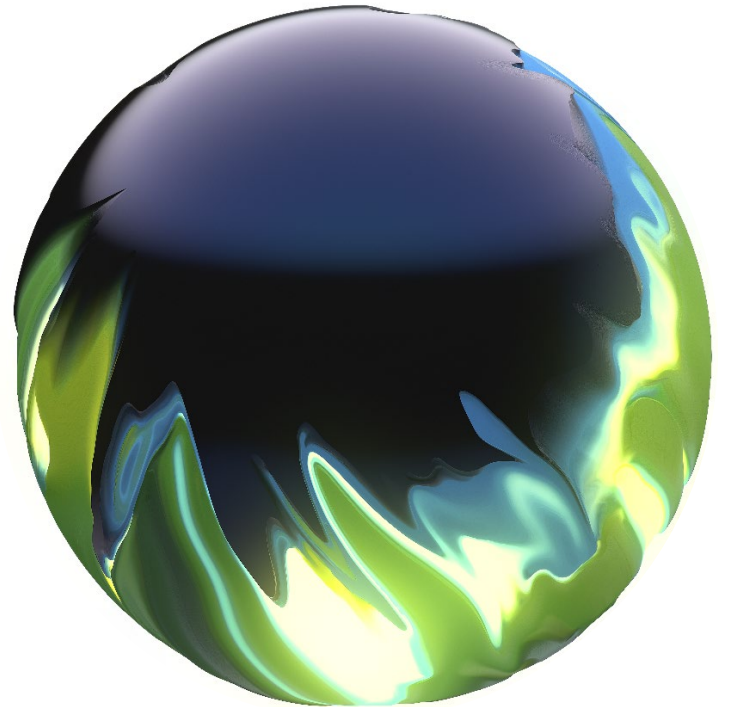
Ransomware attacks are on the rise, with increasing persistence and sophistication by threat actors who are adept in evasion techniques. On Friday 7 May, a ransomware attack was reported by the largest gasoline pipeline in the United States. And they paid nearly \$5 million in bitcoin for the encryption key. While the pipeline is fully operational now, many US gas stations were still without fuel two weeks later. On 14 May, ransomware took down Ireland's health service's IT systems, which left most of the country's hospitals without computers for over a week. That means medics had limited or no access to patients' records, among other critical impacts. The most recent attack on global food producer JBS shut down operations around the world.

These attacks on industrial, utilities, and life sciences and healthcare companies continue to grow in frequency and impact, leading industry experts to warn that failing to address key cybersecurity concerns may have even more devastating consequences in future attacks, to both economies and to critical infrastructure.

Every organization is vulnerable to ransomware attacks. Ransoms are paid because the cost is less than rebuilding the IT infrastructure based on the most recent backups. Organizations should be continually monitoring their processes that have access to sensitive data. Access control and data encryption management is the key to securing an organization – not only from ransomware, but from insider threats, rogue processes, malware and more. **It's vital that the CEO and the board are fully equipped with the knowledge to deal with the prospect of a ransomware attack hitting their organization and are doing as much as possible to ensure this doesn't happen.**

When there's accessibility to valuable data, attacks will occur

Next-generation disruptive technologies from ransomware attackers are making it increasingly difficult to reduce the attack surface.



Organizations that don't mitigate that part of the hacker's modus operandi are opening themselves up to costly and sometimes catastrophic consequences. Strong cyber hygiene practices should be prioritized, regardless of industry, to reduce the threat of ransomware attacks, which includes workforce training on sound cyber practices.

To complicate an adversary's efforts to identify points of weakness between interconnected networks, development environments and cloud-enabled services, organizations should also consider a Zero Trust framework whereby users are granted access to a network service for a specific task and must reauthenticate for new tasks, and where continuous monitoring for anomalous activity is in place. Security planning should also reflect zero trust principles within the enterprise and software lifecycle to eliminate implicit trust in any network node or access point.

In an urgent memo on 2 June to American organizations, the Biden administration is urging corporate executives and business leaders to take immediate steps to prepare for ransomware attacks. On 12 May in the aftermath of the pipeline attack, US President Biden signed a cybersecurity executive order creating guidelines for responding to such attacks, mandating transparency by companies who have been attacked and increasing governmental involvement in the aftermath of any exploitation. The recent attacks continue to highlight the opportunity and importance for governments and the private sector to engage in more effective information sharing.

Cybercrime is not just a crime against a computer but against trust and the impacts are far reaching. Ransomware attacks are not going away any time soon, which means everyone has to get better at preventing a targeted attack from becoming a successful one.









What will you do?

A new precedent in ransomware attacks



Global businesses are expected to face a ransomware attack **every 11 seconds**, costing targets an estimated **USD \$20 billion** (Source: Cybersecurity Ventures).

Common security challenges make organizations susceptible to ransomware

 Lack of segmentation of OT and IT networks to confine an attack from expanding into critical networks and control systems	 Limited awareness of attack surface vulnerabilities and paths to critical systems and assets
 Lack of redundant backups that have been tested for resiliency and business recovery effectiveness	 Lack of modern tools to provide remote and administrative access to OT systems, such as multi-factor authentication
 Inadequate vulnerability management and lack of broad and efficient patching cycles and testing	 Lack of ransomware incident response plans to bring critical systems back online and enable business continuity
 Limited ability to monitor for anomalous uploads through user and entity behavioral analysis (UEBA) and data loss prevention (DLP) tools	 Limited coordination between OT and IT, leading to siloed views of cyber threats and segregated incident response and resiliency plans

Are you confident in your ability to respond to a ransomware attack?

- Are you identifying all your IT and OT assets and their associated risks, vulnerabilities, and patching?
- Do you have appropriate visibility into potential threats targeting your environment and adequate telemetry & analytics to identify suspicious and potentially malicious activity across the enterprise?
- How prepared is your organization to recover from a ransomware incident and follow your crisis plan?
- Are you mapping your cyber footprint so you can look at it from an attacker's perspective and identify potential vulnerabilities?

Steps to improve cyber posture



Proactively plan for a crisis: Prepare for technology disruption scenarios (including cyber incidents) with emphasis on security governance, strategic risk management, and supporting policies to effectively monitor and measure risk.



Map out your most critical systems and assets: Identify assets critical to your operations which could appeal as targets for threat actors by mapping out your attack surface and maintaining a current inventory of assets continuously scanned for vulnerabilities.



Prevent compromise of IT from spreading to OT: Segment your critical systems and OT network, deploy advanced monitoring for suspicious activity, and use jump-boxes to further control access.



Accelerate your adoption of Zero Trust: Assume breach and remove implicit trust from users, workloads, networks, and devices. Protect administrative credentials with layered access controls and prioritize network segmentation as well as telemetry & analytics.



Increase resiliency of your business: Place as much importance on response efforts, telemetry and analytics as prevention and detection including business resiliency planning, and simulation exercises.



Go on offense: Modern security principles such as proactive threat hunting, machine learning cyber analytics, and self-healing systems can help you take an offensive approach.



Perform a Ransomware Preparedness Assessment: Evaluate your cybersecurity program for preparedness, response and recovery with respect to ransomware attacks to identify strategy and capabilities gaps.

Our diverse and experienced team of Cyber professionals consulting over 10 consecutive years are well-positioned globally to ensure local points of contact and to provide our solutions and offerings with unmatched consistency and quality of execution.

Deloitte Cyber | Empowering your people for the future

9.5K

of cyber engagements in FY2020 across all major industries

80%

Share of FG500 companies that we serve

\$3.5B

Global Security Consulting revenue

The Deloitte Difference

In this digital world, your reputation begins and ends with cyber. As a worldwide leader in cyber strategy consulting and cyber intelligence, Deloitte offers a fully customizable suite of cyber solutions and managed services.

With a commitment to technological innovation and broad industry expertise, our Deloitte global network gives us the insight and experience to face any scenario. Because we listen to your needs, Deloitte Cyber is uniquely equipped to help you navigate the evolving landscape for a successful future.

Cyber Capabilities



22,000 Cyber practitioners worldwide



30+ Years in providing Cyber Risk Capabilities



We advise, implement and operate a comprehensive portfolio of cyber solutions and services to your current industry sector requirements and enterprise-wide needs to anticipate and prepare for the cyber risks of the future



2,000+ certified information systems security specialists globally

Accolades



Ranked #1 globally in Security Consulting, 10 consecutive years based on revenue by Gartner¹



Deloitte named a leader in Managed Security Services 2020 Vendor Assessment²



Deloitte named a global leader in Cybersecurity Consulting by ALM³

¹Source: Gartner, Market Share: Security Consulting Services Worldwide, 2020, Elizabeth Kim, April 2021

²Source: IDC MarketScape: Worldwide Managed Security Services 2020 Vendor Assessment by Martha Vazquez, September 2020, IDC #US46235320e

³Source: ALM Intelligence; Cybersecurity Consulting 2019; ALM Intelligence estimates © 2019 ALM Media Properties, LLC. Reproduced under license

Note: Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Authors and contacts



Emily Mossburg | Global Cyber Leader

+1 571 766 7048

emosburg@deloitte.com



James Nunn-Price | Asia Pacific Cyber Leader

+61 293 227 971

jamesnunnprice@deloitte.com.au



Amir Belkhelladi | Canada Cyber Leader

+1 514 393 7035

abelkhelladi@deloitte.com.ca



Peter Wirnsperger | Central Europe Cyber Leader

+49 403 208 04675

pwirnsperger@deloitte.de



Simon Owen | North and South Europe Cyber Leader

+44 20 7303 5133

sxowen@deloitte.co.uk



Deborah Golden | United States Cyber Leader

+1 571 882 5106

debgolden@deloitte.com



Nicola Esposito | Global Cyber Detect and Respond Leader

+134 918 232 431

niesposito@deloitte.es

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see <http://www.deloitte.com/about> to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the “Deloitte organization”) serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 330,000 people make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.