Deloitte.

# Defending against ransomware in an age of emerging technology

In 1989, an AIDS researcher and evolutionary biologist named Joseph Popp mailed floppy disks to researchers around the world who were attending the World Health Organization's AIDS conference that year. When the researchers inserted the disks into their desktops, they thought they were going to learn about a methodology for determining patients' risk of contracting AIDS. Instead, they got a computer virus that is widely regarded as the first example of ransomware.[1]

Ransomware has come quite a long way since then, much to the chagrin of security professionals, and it shows no sign of abating. Its cost is expected to exceed $265 billion over the next 10 years, and it has gained such worldwide notoriety that, in June 2021, US President Joseph Biden identified ransomware as an escalating and shared global threat that requires a collective response from the government and private sector.[2]

For security professionals seeking to address current and future ransomware risks, looking back at ransomware events of the past can provide valuable lessons. Here, we explore ransomware trends; the impact of emerging technologies on the evolution of ransomware and defenders' ability to prevent and detect these attacks; and steps organizations can take to keep ahead of this threat.

## Understanding the impact: Current trends and implications

- Threat actors increasingly use access brokers—cybercriminals who sell stolen information, such as endpoint URLs, login credentials, and IP addresses—to gain initial access to organizations.
- Ransomware malware can now evade antimalware tools, which makes it harder for defenders to detect.
- Once on a victim's network, attackers leverage persistence techniques to maintain access and make it harder for defenders to kick them off.[3]
- Attackers leverage advanced encryption technology to get around victim organizations' efforts to rapidly decrypt data encrypted during attacks.
- Adversaries employ a variety of tactics to put even more pressure on victims to pay ransoms, including:
  - Intentionally targeting their data back-up environments, rendering organizations' recovery plans obsolete
  - Combining ransomware attacks with distributed denial-of-service (DDoS) attacks that further disrupt victims' business operations[4]
  - Threatening to publicly release victims' data (data extortion)
  - Using vulnerabilities in supply-chain networks to access a large number of victims and paralyze multiple networks simultaneously
- Ransomware-as-a-Service (RaaS) platforms contribute to increases in attacks by lowering barriers to entry for attackers and allowing more people, including those who are less tech savvy, to collaborate and exploit already developed malware.[5]

## Disrupting business: From a cybersecurity nuisance to an enterprise-wide risk

### Ransomware then (1989 – 2016)

In the early days of ransomware, the tactics, techniques and procedures (TTPs) that threat actors used were rudimentary, and ransomware was more of a nuisance than a prominent cyber threat.

**1989** – The first act of ransomware takes place.[6]

**2005** – Cybersecurity researchers record the first known ransomware variant in the wild.

**2011** – Anonymous payment methods lead to the first largescale proliferation of ransomware malware.

**2013** – Ransomware code named CryptoLocker appears and uses bitcoin and encryption for the first time. Bitcoin helps to transform ransomware into a lucrative business for cybercriminals; using bitcoin to pay ransoms becomes the norm and attracts a growing number of threat actors.[7]

### Ransomware now (2017 to present)

Over the past few years, the TTPs ransomware actors use have evolved, and their attacks have become more sophisticated, costly, and disruptive. Ransomware has become a significant threat that poses risks to the business continuity of entire organizations.

**2017** – NotPetya masks destructive malware as ransomware and leads victims to think paying the ransom will facilitate recovery, but it does not because no decryption key is available. The attack causes long-term operational disruptions across large international organizations, demonstrating it poses high enterprise-wide risk.[8]

**2018** – Ransomware group Ryuk forms and launches the first known targeted ransomware attack which becomes the norm.

**2021** – Within weeks, ransomware hits the largest fuel supplier on the US east coast, the world's largest meat processing company, and in a single separate attack about 1,500 businesses; these attacks affected business operations and demonstrate the potential for massive disruption across industries and the enterprise-wide risk that ransomware now poses.[9]

# Changing the game: Impact of emerging technologies on adversaries and defenders


## Internet of Things (IoT) and 5G

IoT platforms and 5G networks appear to give more advantages to adversaries than to defenders, and both technologies pose similar cybersecurity risks to organizations.

### Impact for adversaries

IoT devices and 5G networks **expand organizations' attack surfaces** and provide threat actors with **more entry points into organizations**. They also create **more data for ransomware actors to seize**, and since industrial IoT devices collect data that could be more detailed, sensitive, or otherwise critical to the victim organization, ransomware attacks targeting IoT devices or data could be **more disruptive**. Moreover, if ransomware actors can gain access to data collected by personal IoT devices, like **home voice assistants**, they can then use that data to craft ever more convincing spear-phishing emails to **perpetuate attack cycles**.

### Impact for defenders

Given the ransomware risks IoT devices and 5G networks create, defenders will need to integrate **security technology, secure design principles, and governance** at each stage of their organization's IoT and 5G deployments and in each layer of their IoT architectures.

## Quantum computing

Both adversaries and defenders can benefit from advancements in quantum computing, which may reach maturity in as few as five years.

### Impact for adversaries

Future quantum computing breakthroughs can drastically **accelerate decryption of data** encrypted with current encryption protocols, such as Transport Layer Security (TLS) or its predecessor Secure Socket Layer (SSL).[10] Hence, if ransomware groups possess fault-tolerant quantum computers and gain access to victims' networks, they could potentially decrypt network communications and other data encrypted with these older protocols **within hours or seconds**.

### Impact for defenders

Just as adversaries may be able to use quantum computing to decrypt data encrypted with current protocols, so too, could defenders. Detection algorithms could be enhanced with quantum technology to **facilitate identification and decryption of encrypted malware**. Defenders can also use quantum computers to decrypt threat actors' communications to **enable proactive monitoring**. They may even be able to **disrupt the ransomware attack cycle** by leveraging quantum to **liberate data** that ransomware actors have encrypted using TLS or SSL.

## Artificial Intelligence (AI)

Adversaries and defenders alike use AI and its offshoot, machine learning, to achieve their objectives and are likely to step up their adoption of these technologies in the years ahead.

### Impact for adversaries

Attackers are using AI to mount **more automated, aggressive, and coordinated campaigns**. For example, they use AI and machine learning to collect personal information from social media sites and automatically generate highly effective phishing emails and fake social media posts; to conceal malicious code in benign applications; and create **malware capable of mimicking trusted system components**.

### Impact for defenders

Defenders can use AI to perform continuous, extensive, and **real-time monitoring of hacker forums** on the open, deep, and dark web, where ransomware actors discuss potential targets and buy stolen credentials to use in their operations. By automatically monitoring the internet for such discussions, defenders can more proactively **pick up on early attack warning signs**.

IoT and 5G pose challenges for cyber defense, while AI and quantum computing may provide defenders with tools they can use to outmaneuver adversaries.

# Mitigating the risks: Enterprise response for ransomware risks

Ransomware attacks now pose not only a cybersecurity but also an enterprise-wide risk, threatening business continuity and the operations of entire organizations. Therefore, to mitigate their effects, organizations should consider implementing solutions to enhance cyber resilience and remediate enterprise risk.

- Assess and integrate the risk of ransomware attacks into enterprise risk and crisis management procedures.
- Implement an offline and secured cyber recovery vault to protect mission critical data, applications, and business services.
- Create a ransomware playbook that details your incident response plan in the event of a ransomware attack
- Conduct cyber wargames to simulate attacks and practice your organization's response.
- Continuously map and understand your organization's attack surface, including all critical assets and systems.
- Constantly monitor the cyber threat landscape and evolving threats, including those that exploit third-party relationships.
- Maintain strict password and user authentication policies and introduce multi-factor authentication across the organization.
- Implement and regularly update cyber threat awareness and education programs for employees and third parties; these programs should include training on social engineering and phishing emails.

## Strategic difference with Deloitte Cyber & Strategic Risk: Transforming cyber resilience

Deloitte can help clients design, build, and operate dynamic, business-aligned security programs wherever they may be in their cyber journey. Services related to ransomware response include, but are not limited to, the areas noted below.

We combine industry-leading strategic advisory services with deep technical capabilities and managed services to help organizations design, implement, and operate advanced cyber and strategic risk programs that build resiliency, deepen trust and fuel performance.

- Ransomware Readiness Assessment
- Cyber Resiliency & Recovery Planning
- Crisis Management & Risk Management
- Threat Hunting & Intelligence
- Attack Surface Management
- OT Security Architecture
- Zero Trust Transformation
- Identity & Access Management (IAM)
- Threat Detection & Response
- Incident Response Retainers & Forensics
- User Behavior Analytics (UBA) Monitoring
- Red Teaming & Penetration Testing
- Breach & Attack Simulations
- Supply-chain Risk Management
- Infrastructure Risk Management

**#1 globally in security consulting in Gartner Market Share report since 2012[11]***

**Leader in the IDC MarketScape: Worldwide Managed Security Services 2020 Vendor Assessment[12]**

**24x7 global cyber threat intelligence capability; 900+ certified specialists (CISSP, CEH, CISA, etc.)**


**Deborah Golden**
US Cyber & Strategic Risk Leader
Deloitte & Touche LLP
Tel: + 1 571 882 5106
Email: debgolden@deloitte.com

**Kieran Norton**
US Cyber & Strategic Risk Infrastructure Leader
Deloitte & Touche LLP
Tel: + 1 415 783 5382
Email: kinorton@deloitte.com

**Curt Aubley**
US Cyber & Strategic Detect & Respond Leader
Deloitte & Touche LLP
Tel: +1 831 515 9797
Email: caubley@deloitte.com



1. Ronny Richardson and Max M. North, "Ransomware: Evolution, Mitigation and Prevention" (2017). Faculty Publications. 4276, p. 11.
2. The White House, "FACT SHEET: G7 to Announce Joint Actions on Forced Labor in Global Supply Chains, Anticorruption, and Ransomware," June 13, 2021; . David Braue, "Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031," Cybercrime Magazine, June 3, 2021
3. Ransomware Task Force, "Combating Ransomware: A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force," Institute for Security and Technology, 2021; MITRE, Ransomware Techniques in ATT&CK; Internet Crime Complaint Center (IC3), "Ransomware: What It Is & What To Do About It," February 4, 2021
4. Sean Newman, "How Ransomware is Teaming Up with DDoS," InfoSecurity Magazine, June 18, 2021
5. Ransomware Task Force, Combating Ransomware: A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force, Institute for Security and Technology, 2021.
6. Ronny Richardson and Max M. North, "Ransomware: Evolution, Mitigation and Prevention" (2017). Faculty Publications. 4276, p. 11.
7. Ronny Richardson and Max M. North, "Ransomware: Evolution, Mitigation and Prevention" (2017). Faculty Publications. 4276, p. 11-12
8. Kim S. Nash, Sara Castellanos and Adam Janofsky, "One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs – WSJ," Wall Street Journal, June 27, 2018.
9. Jacob Bunge and Jesse Newman, Ransomware Attack Roiled Meat Giant JBS, Then Spilled Over to Farmers and Restaurants," Wall Street Journal, June 11, 2021; Deloitte, "How resilient is your critical infrastructure against cyberattacks?," June 2021; Meghan Bobrowsky, Kaseya Ransomware Attack: What We Know as REvil Hackers Demand $70 Million," Wall Street Journal, July 6, 2021
10. Scott Buchholz, Deborah Golden, Caroline Brown, "A business leader's guide to quantum technology" Deloitte Insights, April 15, 2021
11. Gartner, "Market Share: Security Consulting, Worldwide, 2020, " Elizabeth Kim, 6 April 2021. Market share based on revenue.

*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.

12. Martha Vazquez, IDC, "IDC MarketScape: Worldwide Security Services 2020 Vendor Assessment" (Doc # US46235320), September 2020