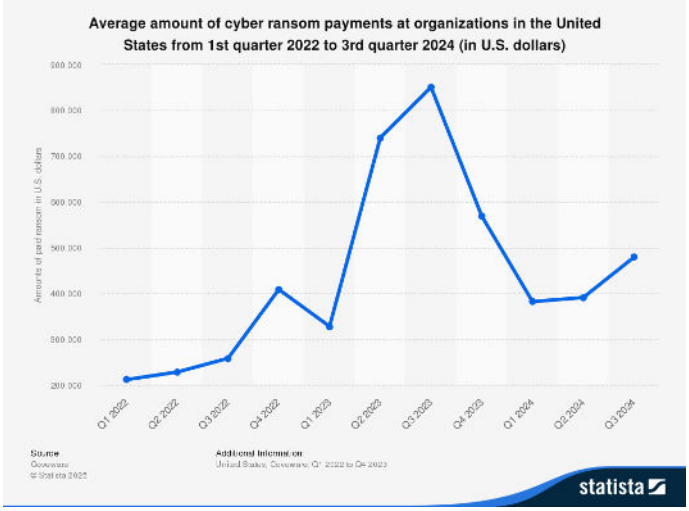
graylog

# Ransomware Payment Guide

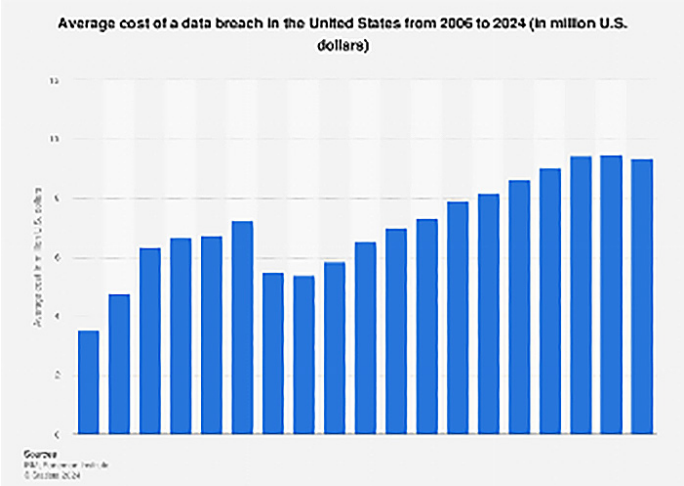
Ransomware threatens organizations worldwide, with criminals setting demands to maximize payouts from those least able to endure disruptions. The growing ransomware threat is pushing authorities to rethink their approach. Countries around the world are implementing plans to limit funds reaching ransomware criminals in different ways. For example, while in the UK, ministers have considered a ban on all UK public bodies making ransomware payments, the Australian government chose to focus on prevention, employee hygiene, and post-incident support.

**"Ransomware attacks have surged globally, which has led to an increased number of ransomware payments. But it must be remembered that, even with the rising number of attacks, paying the ransom does not guarantee data recovery. Moreover, paying ransomware fuels the ransomware business model. Law enforcement agencies strongly advise against paying ransoms, as it encourages further criminal activity and offers no assurance of data restoration."**

*Use this guide alongside a robust incident response plan. An effective ransomware risk management requires proactive investment in both prevention and response. The guide focuses on framing the right decisions during an attack.*




**Average amount of cyber ransom payments at organizations in the United States from 1st quarter 2022 to 3rd quarter 2024** *(in U.S. dollars)*




**Average cost of a data breach in the United States from 2006 to 2024** *(in million U.S. dollars)*

**Sources: Statista**
https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach/
https://www.statista.com/statistics/1409510/ransom-payment-us-quarterly-amount/

# State of Play

Ransomware, a type of malicious software that encrypts data and demands payment for its release, is an escalating global threat. It affects both private organizations and public services. In 2024, 59% of organizations worldwide reported falling victim to ransomware attacks, according to a survey among cybersecurity leaders.

The good news is that the total amount paid in ransomware attacks decreased by more than a third in 2024 to $813 million, down from $1.25 billion in 2023. But with cybercriminals now embracing AI, attacks are becoming more frequent and sophisticated. AI enables attackers to automate phishing attempts, personalize fraudulent communications, and adapt tactics in real-time, making traditional security measures less effective.

Beyond the statistics, ransomware attacks on the public sector including healthcare can have life-threatening consequences. When critical systems like ambulance dispatch or patient care records are compromised, the damage goes far beyond financial loss, and lives can be at risk. Addressing ransomware is therefore not only a matter of cybersecurity but also one of public safety.

# What factors should you consider before deciding whether to pay the ransom?

Paying the ransom or refusing carries inherent risks, and the decision to pursue either option should be guided by expert advice, including legal counsel specific to the situation. The decision should also consider whether the current circumstances involve unacceptable or potentially catastrophic impacts.

## 1. Risk to Life and Safety:

Does paying the ransom reduce risks to life, safety, or critical infrastructure? If there are significant life-threatening consequences, paying may be the most responsible action.

## 2. Survivability of the Organization:

Can the organization survive the costs or other impacts of the cyber incident without paying the ransom? If the financial or operational damage is too severe, paying might be the only viable option to ensure survival.

## 3. Ethical Considerations:

Consider the broader impact of the decision. Is paying in the interest of a "greater good," such as protecting vulnerable individuals, communities, or other stakeholders? This includes considering the interests of individuals whose information is at risk, shareholders, or other affected parties.

## 4. Legal Implications:

Assess whether paying the ransom is unlawful. Paying might violate local laws, sanctions, or regulations, depending on the jurisdiction or the actors behind the attack. It is important to understand the potential legal consequences of making the payment.

## 5. Long-Term Impact:

Will paying the ransom set a precedent, potentially making the organization a target for future attacks? This can affect the organization's long-term security posture and reputation.

## 6. Potential for Recovery:

Is there a possibility of recovering the data or systems without paying the ransom (e.g., through backups or other means)? Weighing the potential costs of recovery without payment should be a factor in the decision.

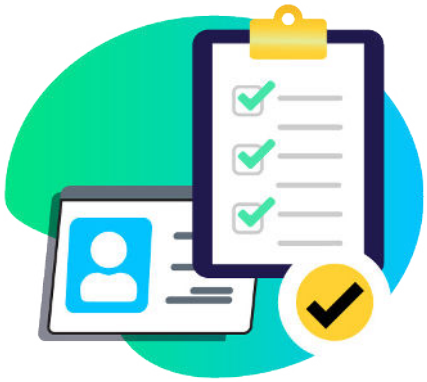
## 7. Expert Advice:

Seek expert counsel, including legal, cybersecurity, and negotiation professionals. They can provide a clearer understanding of the risks and implications associated with paying the ransom.

By considering these factors, the decision to pay the ransom can be made with a clearer understanding of the associated risks and responsibilities.

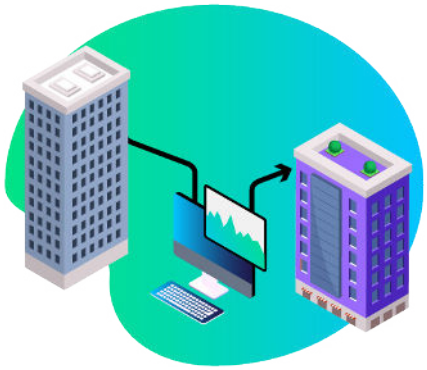
# Now, what steps should you need to take when things go wrong and your organization is under attack?

## 1. Immediate Incident Response Steps



- **Isolate Affected Systems:** Disconnect infected systems from the network to prevent further spread.
- **Identify the Scope:** Determine which systems and data have been compromised.
- **Preserve Evidence:** Document affected systems, ransom notes, and network activity for forensic analysis.
- **Notify Stakeholders:** Inform IT security, legal teams, senior leadership, and, if necessary, law enforcement.

## 2. Assessing Backup and Recovery Options



- **Verify Backup Integrity:** Confirm recent backups are available and not compromised.
- **Restore from Backup:** If possible, use secure backups to restore operations.
- **Explore Recovery Methods:** Consider third-party decryption tools or expert cybersecurity support.

## 3. Engaging Law Enforcement and Cybersecurity Experts

- **Report the Attack:** Notify law enforcement and cybersecurity agencies for guidance.
- **Consult Experts:** Work with cybersecurity firms to assess threats and recovery options.
- **Conduct Forensics:** Investigate the attack's origin, exploited vulnerabilities, and ongoing risks.

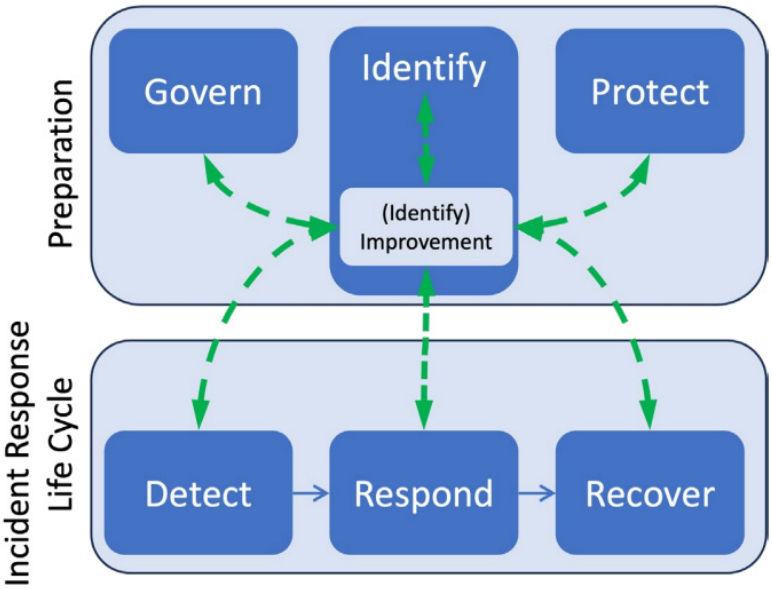
## 4. Evaluating Legal and Regulatory Considerations

- **Review Compliance Obligations:** Check if data protection regulations require breach notifications.
- **Assess Legal Risks of Payment:** Understand the legal consequences of paying ransom, including potential sanction violations.
- **Consult Legal Counsel:** Seek advice on regulatory compliance and liability.

## 5. Strengthening Future Defenses

- **Implement Backup Strategies:** Ensure secure, encrypted, and regularly updated backups.
- **Strengthen Security:** Use advanced threat detection, endpoint protection, and employee cybersecurity training. Develop a Ransomware Response Plan: Create a documented plan to streamline future responses.
- **Conduct Regular Audits:** Identify vulnerabilities and apply necessary security updates.

**Incident Response Lifecycle Model**




**Sources:**
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.ipd.pdf
https://graylog.org/post/creating-an-incident-response-process/

## Conclusion:

**Checklists to help security teams organize incident response processes.** Graylog Security maps events to the MITRE ATT&CK Framework using prebuilt content;

- Combine Sigma rules with MITRE ATT&CK to create alerting rules for threat detection, investigation, and threat hunting.
- Monitor user activity for anomalies and map to MITRE ATT&CK to detect Initial Access attempts through Valid Accounts, isolating compromised accounts early.


Graylog's risk scoring aggregates log severity with asset details, reducing alert fatigue and focusing security teams on high-risk issues.

**Request a Graylog Demo**

## ABOUT GRAYLOG

Graylog is the no-nonsense SIEM that cuts through noise and complexity. It delivers what security teams need most: full visibility, faster investigations, and smarter detection—without trade-offs or surprise costs. From automated workflows to correlation and anomaly detection, Graylog helps analysts move faster and stay focused. With a product suite spanning Graylog Enterprise, Security, API Security, and Open, we support everyone from large enterprises to lean teams. Trusted by over 60,000 organizations around the world. Learn more at graylog.com or connect with us on Bluesky and LinkedIn.

www.graylog.org
info@graylog.com | 1301 Fannin Street, Suite 2000, Houston, TX 77002