ASIA PACIFIC | SINGAPORE

Ransomware:

How to manage the risk

AIG®

For full pdf features, please view in Adobe Acrobat.

Ransomware: what it is and how it works

What is Ransomware?

Ransomware is malicious software that gets inside files or systems and then blocks access to them. The affected files, or even entire devices, are then held hostage using encryption until the victim pays a ransom in exchange for a decryption key that allows the user to access the encrypted areas.

How it works

Ransomware has to access files or systems to hold them to ransom. They may take the form of email attachments, social media messages and pop-ups, to trick recipients into opening them in order to access and lock down connected files, networks or systems.

Possible impacts

A ransomware infection can cause loss of sensitive data, operational disruption, reputational damage and financial loss. Paying a ransom does not guarantee the release of encrypted files and may actually disclose the victim's banking details. Even decryption does not mean the malware infection has been removed.

Major Ransomware attacks

Ransomware continues to dominate the cybersecurity landscape, with businesses large and small paying millions of dollars to unlock encrypted files. Some of the severest known ransomware attacks so far include: NotPetya (2017), WannaCry (2016), Petya (2016), LOcky (2016), CryptoWall (2014), CryptoLocker (2014).

Ransomware for sale

Cybercriminals have set up professional affiliate programs providing payment for distributing malware. The developers of the so-called GandCrab ransomware strain announced in 2019 that they were terminating the program after allegedly earning more than $2 billion in extortion payouts from victims.

Managing the risk of ransomware infection

The US National Institute of Standards and Technology's Cybersecurity Framework includes five high level functions for preventing and managing a ransomware attack: Identify, Protect, Detect, Respond and Recover.

We have used this framework to develop a systematic process to help our clients prevent and manage ransomware attacks, including the AIG CyberEdge pre-loss services.

Preventing infection:

IDENTIFY

Preventing infections from happening starts with identifying:

- The organisation's physical and software assets and the business environment that the organisation supports, such as its role in the supply chain and place in the critical infrastructure sector.
- Asset vulnerabilities, threats to organisational resources, and risk response activities.

These need to be considered for the entire asset inventory including unmanaged devices in relation to the reliability, availability and serviceability of the IT and OT.

AIG and our partners can help clients with the identification process with our range of complimentary* pre-loss services

Measure and monitor network security

Security ratings are available for organisations to measure and monitor their own network. The ratings are generated unobtrusively through continuous measuring of externally observable, freely accessible data.

CyberEdge insureds are eligible to receive complimentary rating reports to measure their own business security performance.

Cyber Maturity Report

Upon completion of the AIG application form, businesses can obtain a comprehensive report providing details of how their controls can be improved to help minimise risk. This report is only available in selected countries.**

Cyber services orientation

CyberEdge customers will receive a one-hour remote session with an AIG Risk Consultant to address questions regarding the Cyber Maturity Report and discuss complimentary services available.

Preventing infection:

PROTECT

Effective protection means implementing a set of protective processes and procedures to maintain and manage the security of information systems and assets. Different aspects should be considered, including:

- The patching of IT and OT.
- The creation and testing of online and offline data and system information backups, stored in different locations.
- Network segmentation and system hardening.
- Staff empowerment through awareness and training, including role-based and privileged user training.

AIG and our partners can help clients implement protection with our range of complimentary* pre-loss services

Employee cybersecurity eLearning

Timely and relevant eLearning courses tailored to employees' roles to reinforce cybersecurity best practices.

Blacklist IP blocking and domain protection

Enables organisations to control their exposure to criminal activity by leveraging vast threat intelligence repositories, precision geoblocking and blacklist automation to reduce risk. Reduces the attack surface up to 90% ahead of the firewall.

Preventing infection:

DETECT

Detecting anomalies and events is the third step to successfully preventing malware infections. This includes:

- Implementing security continuous monitoring capabilities to monitor cybersecurity events and verify the effectiveness of protective measures, including network and physical activities.
- Maintaining detection processes to provide awareness of anomalous events.

Ensuring rapid detection starts with establishing a Security Information and Event Management (SIEM) or even a Security Operation Center (SOC) functions with strong threat intelligence. Having clear network and endpoint visibility helps your organisation to make the detection easier.

AIG and our partners can help clients detect potential events with our range of complimentary* pre-loss services

Infrastructure vulnerability scan

- Identify, quantify and classify the security vulnerabilities within your computing environment by using scan engines.
- Scan up to 250 IP addresses.
- Identify current vulnerabilities and false positives.
- Vulnerability assessment report will include three business days of scan or post analysis support.
- Perform a reassessment scan within 90 days of original.

Phishing simulator

Part of the eLearning tool, the phishing simulator delivers real world scenarios to reinforce learning and remediate behaviors. Identify susceptible users and compare performance over time.

RESPOND

before and after an infection

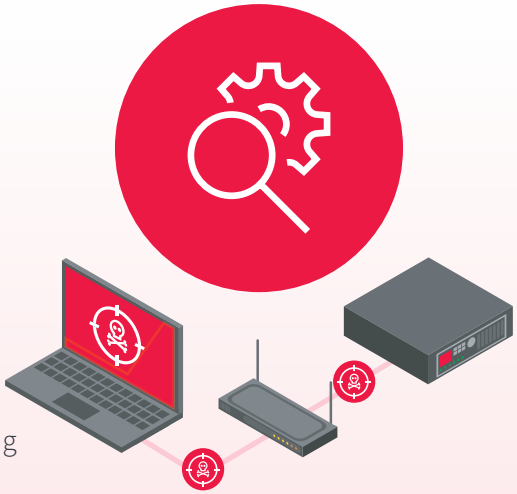
Before an infection, a well-developed response mechanism within the organisation helps to mitigate the potential damage during a ransomware infection. This can include:

- Performing mitigation activities to prevent expansion of an event and to resolve the incident.
- Implementing improvements by incorporating lessons learned from current and previous detection or response activities.

All this requires a Cyber Security Incident Response Team (CSIRT) that has developed and established a tested Incident Response Plan.

After an infection reactive measures must be initiated, including:

- Ensuring response planning processes are executed during and after an incident.
- Managing communications during and after an event with stakeholders, law enforcement agencies, and external stakeholders as appropriate.
- Conducting analysis to ensure effective response and support recovery activities, including forensic analysis, and determining the impact of incidents.



AIG and our partners can help clients with the response process as part of our claims support

AIG Cyber Claims Hotline

Our CyberEdge Claims Hotline is available 24/7/365.

In helping you implement your response plan, the Cyber Claims Team will coordinate any necessary vendors to implement your response plan, engage any necessary vendors including breach counsel and forensics firms to identify immediate threats, and start the restoration and recovery process.

Incident Response: Forensic

As part of the CyberEdge policy's incident response, get access to forensic experts to investigate, secure and recover from an incident.

Incident Response: Legal

As part of the CyberEdge policy's incident response, get access to legal experts who provide strategic direction over the event, advice in relation to regulatory and legal obligations, and provide client confidentiality over information relating to the incident.

Incident Response: Public Relations

As part of the CyberEdge policy's response, get access to communications experts to guide on crisis communications and handling of media.

RECOVER
after a ransomware attack

For optimum business recovery after a cybersecurity attack, it is essential to execute plans for resilience and restore any capabilities or services that were impaired due to the incident. Timely recovery to normal operations will reduce the impact of a ransomware infection.

Organisations need to implement recovery planning processes and procedures to restore systems and/or assets affected by Cybersecurity incidents and recover data from (offsite) backups.

AIG and our partners can help clients in the recovery process as part of our claims support process

Data recovery
CyberEdge's incident response cover gives clients access to experts to restore, recreate, repair or recollect lost, damaged, destroyed, encrypted or corrupted data and systems.

Cyber extortion services
Get access to an extensive range of specialist services to combat the use of ransomware for cyber extortion. The CyberEdge incident response process includes conducting investigations to validate a threat, containment and negotiations to end an extortion event, through to ransom payments.

Network interruption
The CyberEdge policy can provide for loss of income, mitigation expenses and forensic accountant costs to quantify the loss when business operations are interrupted by a ransomware incident.

* AIG may modify (by adding, removing or replacing a tool or service) or discontinue a service at any time. AIG may partner with third party vendors to provide any or all of the services.

Service Offering	Annual CyberEdge Premium Range $900 - $4,999	Annual CyberEdge Premium Range $5,000+
Network Security Ratings	Group Level only	Group Level + Subsidiaries
Cyber Maturity Report + Cyber Services Orientation**	Report only	Report + Orientation
Blacklist IP Blocking and Domain Protection	-	Yes
Employee Cybersecurity eLearning	Up to 50 employees	Up to 10,000 employees
Phishing Simulator	-	Up to 10,000 employees
Infrastructure Vulnerability Scan	-	Up to 250 IP addresses
CyberEdge Claims Hotline	Yes	Yes

**For details regarding availability and demos, please discuss with your local AIG underwriter.

Clients can begin the enrolment process by visiting **www.aig.com/cyberlosscontrol** or contact AIG at **CyberEdgeAPAC@aig.com** or your local AIG underwriter.

SINGAPORE
AIG Asia Pacific Insurance Pte. Ltd.
AIG Building, 78 Shenton Way,
#09-16 Singapore 079120

aig.sg