Ransomware:

and how to manage the risk

AIG®

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. Some of the many possibilities include email attachments, social media messages and pop-ups, to trick recipients into opening 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 in 2019, 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 National Institute of Standards and Technology's Cybersecurity Framework includes five high level functions for preventing and managing a ransomware attack: Identification, Protection, Detection, Response and Recover.

To help inform AIG clients and brokers we have used this framework to provide a systematic basis for preventing and managing a Ransomware attack including our AIG CyberEdge pre-loss services.

IDENTIFY

PROTECT

CLICK FOR MORE INFORMATION

RECOVER

DETECT

RESPOND

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 you in this Identification process with our range of complimentary* pre-loss services

Measure and monitor network security

Security ratings 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 will be eligible to receive complimentary rating reports to measure their own business security performance.

AIG Cyber Services Orientation

One hour remote session with an AIG Risk Consultant to address questions around the Cyber Maturity Report and discuss complimentary services available.

Cyber Maturity Report

Available in select countries** and upon completion of the AIG application form, businesses can obtain insights into the cyber risks they face and the threat likelihoods via a comprehensive report including risk reducing qualities of their controls.

Preventing infection:
PROTECT

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

- The patching of IT and OT.
- The creation and testing of online and offline backups of data and system information, 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 you implement Protection with our range of complimentary* pre-loss services

Employee Cybersecurity eLearning
Timely and relevant eLearning courses tailored to employees' roles to reinforce your 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 black-list 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) with good threat intelligence. Having a proper network and endpoint visibility helps your organization to make the detection easier.

AIG and our partners can help you 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/Identify false positives.
- Vulnerability assessment report with three business days of scan/ Post analysis support.
- 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 & compare performance over time.
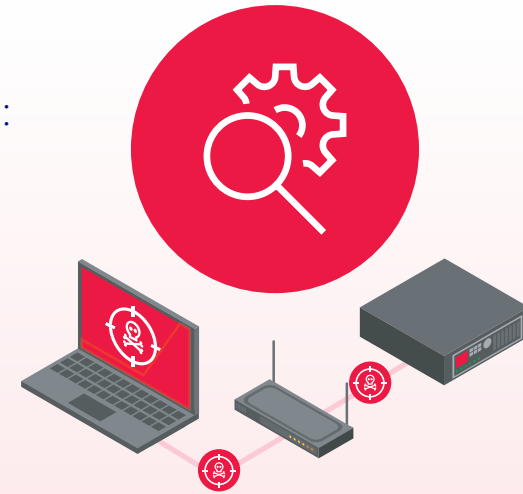
RESPOND
before and after an infection

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

- Mitigation activities that are performed to prevent expansion of an event and to resolve the incident.

- The implementation of 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 process are executed during and after an incident.

- Managing communications during and after an event with stakeholders, law enforcement agencies, external stakeholders as appropriate.

- Conducting analysis is to ensure effective response and support recovery activities including forensic analysis, and determining the impact of incidents.

AIG and our partners can help you in the Response process as part of our claims support

AIG: Cyber Claims Hotline
Our CyberEdge Claims Hotline is available 24/7.
The Cyber Claims Team will coordinate with you 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.

Incident Response: Legal
As part of the CyberEdge policy's incident response, get access to legal experts.

Incident Response: Public Relations
As part of the CyberEdge policy's response, get access to public and communications experts.

RECOVER
after a Ransomware attack

For optimum business recovery after an attack it is essential to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. This supports timely recovery to normal operations to reduce the impact from a ransomware infection.

Organizations have to implement Recovery Planning processes and procedures to restore systems and/or assets affected by cybersecurity incidents and recover from (offsite) backups to restore business operations in a timely manner.

AIG and our partners can help you in the Recovery process as part of our claims support

Data Recovery
As part of the CyberEdge policy's incident response, get access to experts to restore, recreate, repair or recollect lost,damaged, destroyed, encrypted or corrupted data and systems.

Cyber Extortion Services
As part of the CyberEdge policy's incident response, get access to extensive range of specialist services to combat the use of ransomware for cyber extortion. From conducting investigations to validate a threat, to 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 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 RM5,000 - RM19,999	Annual CyberEdge Premium Range RM20,000+
Network Security Ratings	Group Level only	Group Level + Subsidiaries
Cyber Maturity Report + 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.

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