Ransomware:
and how to manage the risk

AIG®

Ransomware: what it is and how it works

What is Ransomware?

Ransomware is malicious software that get's 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.

RECOVER

IDENTIFY

CLICK FOR MORE INFORMATION

RESPOND

PROTECT

DETECT

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 pre-loss services

AIG CyberMatics℠****

AIG's award winning technology-driven process that can help an organization verify its cyber risk posture, prioritize which controls need to change, and better invest in its overall cybersecurity program... which includes the purchase of cyber insurance from an AIG affiliate.

BitSight Technologies***

BitSight generates security ratings for organisations to measure and monitor their own network and those of their third-party vendors. The ratings are generated unobtrusively through BitSight's continuous measuring of externally observable, freely accessible data. CyberEdge insureds will be eligible to receive a complimentary BitSight Security Rating report to measure their business security performance.

AIG Cyber Services Orientation**

One hour with an AIG Cyber Risk Advisor to address questions you may have about your risk posture and recommendations in your cybermaturity reports and to introduce you to AIG's services and key vendor services that can help improve your cyber risk.

Executive Threat Briefing****

AIG Cyber Risk Advisory's Executive Threat Brief is a workshop designed to help your organization better understand the current security threat landscape specific to your industry and current methods attackers are using so that you can better defend your business.

Axio Cyber Risk Quantification****

Exposure quantification is accomplished in a one-day workshop, which can be scheduled as one full day or in several meetings.

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 pre-loss services

TechGuard SHIELD**

Security awareness training for employees including phishing training and simulations. A unique Assess, Educate, Reinforce, Measure training methodology combines the four key components of successful cybersecurity awareness and training programmes. A demo or trial is available upon request.

ThreatBlockr**

ThreatBlockr works together with real-time threat data from AIG to analyze a customer's cybersecurity posture and determine its cyber risk profile with threat and impact scores, benchmarking data and recommended actions for improvement.

Office of the CISO powered by Optiv****

Optiv provides on-demand access to virtual, interim, and staffed CISO expertise as well as critical security advisory services that are tailored to meet the needs of an organisation.

BitSight Technologies***

External Security Rating.

* Free service for CyberEdge customers | ** Free service for CyberEdge customers with a premium higher than €5,000
*** Complimentary access for the insured entity | **** Subject to availability. For details regarding availability, please contact AIG

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 Pre-Loss services:

TechGuard Securities Vulnerability Scan**

- Identify, quantify and classify the security vulnerabilities within your computing environment by using scan engines.
- 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.

Dark Web Intelligence by BlueVoyant****

Summary of Dark Web findings:

- Scans thousands of Dark Web sources, including multilingual forums, cyber black markets, Automatic Vending Machines (AVMs), paste sites, Instant-Messaging / chat platforms and more.
- Gathers information on relevant attackers their plans, methods, and tools and leaked compromised client-relevant information.

RSA NetWitness® Endpoint****

- Integrated Endpoint Detection and Response solution.
- Helps SOC and IT teams to gain insights into the full scope of an attack across both network and endpoint.

BitSight Technologies***

External Security Rating.

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.
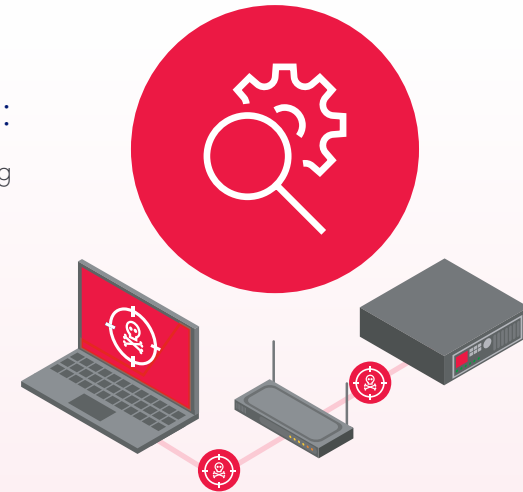
AIG and our partners can help you in the response process with our Pre-Loss services:

RSA Incident Response Retainer****

- IR retainers are proactive cybersecurity measures that can significantly reduce an attacker's dwell time and reduce the impact of a breach.
- IR retainers help your organization to align with the requirements and incentives offered by cybersecurity insurance providers.

Incident Simulation Workshop****

AIG Cyber Risk Advisory's Incident Simulation Workshop is designed to help you ensure your incident response plan will help your organization respond efficiently when a security incident occurs and to better understand the AIG claims process.

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 with cyber incidents as part of our claims support:

AIG: Cyber Claims Hotline*

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

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 incident response, get access to public relations and communications experts.

* Free service for CyberEdge customers | ** Free service for CyberEdge customers with a premium higher than €5,000
*** Complimentary access for the insured entity | **** Subject to availability. For details regarding availability, please contact AIG

AUSTRIA
AIG Europe S.A.
Direktion für Österreich
Herrengasse 1-3
1010 Wien

+43 (1) 533 25 00

BELGIUM
AIG Europe S.A.
Pleinlaan 11
1050 Brussels

+32 2 739 96 20

CYPRUS
AIG Europe S.A.
(Cyprus Branch)
26, Esperidon Street, 2001
Strovolos, Cyprus
P.O.Box 21745, CY-1512
Nicosia

+357 22 699 999

DENMARK
AIG Europe S.A.
Osvald Helmuths Vej 4
2000 Frederiksberg

+45 91 37 53 00

FINLAND
AIG Europe S.A.
Kasarmikatu 44
00130 Helsinki

0207 010 100 (vaihde)

FRANCE
AIG Europe S.A. France
Tour CB 21 16
Place de l'Iris
92400 Courbevoie

01 49 02 42 22

GERMANY
AIG Europe S.A.
Direktion für Deutschland
Neue Mainzer Straße 46 - 50
60311 Frankfurt

+49 (0) 69 97113-0

GREECE
AIG Europe S.A.
119 Kifissias Avenue
15124 Marousi
Athens

210 81 27 600

IRELAND
AIG Europe S.A.
30 North Wall Quay
International Financial
Services Centre
Dublin 1, D01 R8H7

+353 1 208 1400

ITALY
AIG Europe S.A. General
Representation for Italy
Via della Chiusa, 2
20123 MILAN

+39 02.36.90.1

LIECHTENSTEIN
AIG Europe S.A.
Zweigniederlassung
Schaan
Zollstrasse 23 FL-9494
Schaan Fürstentum
Liechtenstein

+423 237 68 81

MALTA
AIG Europe S.A.
98/2, Melita Street
Valletta VLT 1120

356 (21) 238 500

NETHERLANDS
AIG Europe S.A.
Crystal Building B
Rivium Boulevard 216 - 218
2909 LK Capelle aan den
IJssel V Rotterdam

010 - 453 54 55

NORWAY
AIG Europe S.A.
Postboks 1588 Vika
0118 Oslo

+47 22 00 20 20

PORTUGAL
AIG Europe S.A.
– Sucursal em Portugal
Avenida da Liberdade
131 - 3ª
1250-140 Lisboa
+ 351 213 303 360

SPAIN
AIG Europe S.A.
(sucursal en España)
Paseo de la Castellana 216
28046 Madrid

+34 915 677 400

SWEDEN
AIG Europe S.A,
Västra Järnvägsgatan 7, 8tr
111 64 Stockholm

+46 8 506 920 00

SWITZERLAND
AIG Europe S.A.
Sägereistrasse 29
8152 Glattbrugg
+41 (0)43 333 37 00

UK
American International
Group UK Limited
58 Fenchurch Street
London EC3M 4AB

+44 (0)20 7954 7000

Visit www.aig.com or email cyberlosscontrol@aig.com