UK and EMEA

Ransomware:

and how to manage the risk

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 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.

Additional causes can include out of date systems or devices as well as weak and re-used passwords.

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 encourage future attacks. Even decryption does not mean the malicious access has been removed.

Major Ransomware attacks

Ransomware continues to dominate the cybersecurity landscape in 2024, 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).

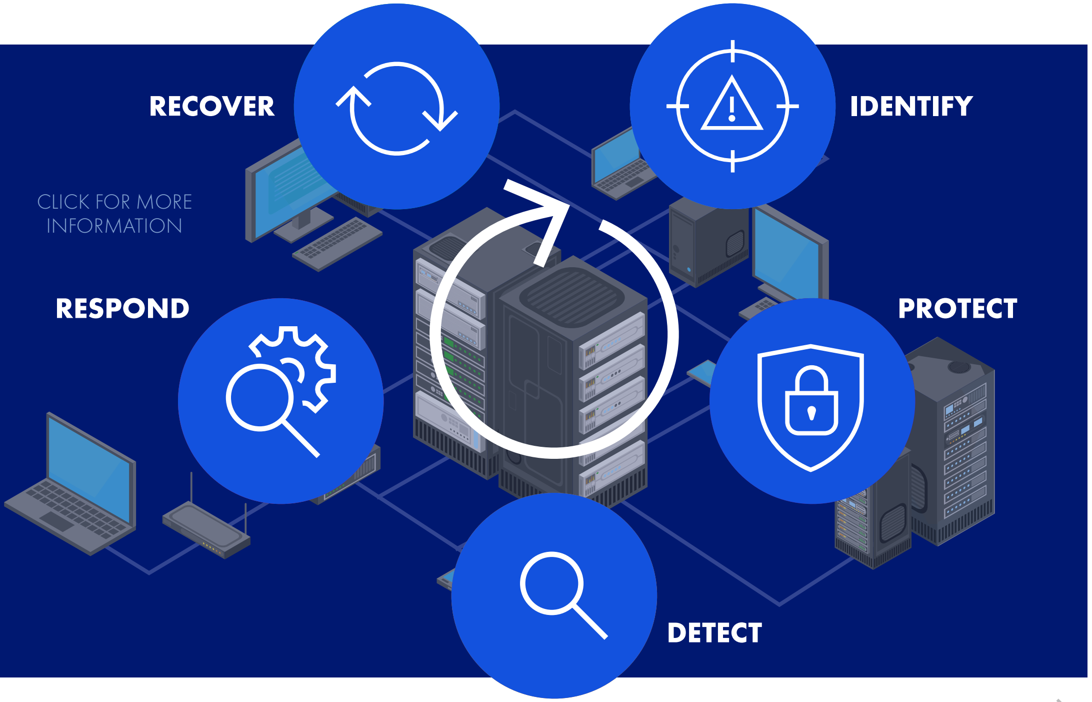
Ransomware for sale

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.



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

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.

Infrastructure Vulnerability Scan from Techguard**

With this annual service, Techguard will help CyberEdge clients identify up to 250 devices or websites with external IP addresses. TechGuard will then scan each of them for weaknesses and provide a detailed report with recommendations to address these weaknesses. Clients can check they have strengthened their infrastructure with a complementary re-scan 90 days later.

Identity Risk Assessment from Silverfort **

Key information, usernames, passwords and permissions are kept in the network's Active Directory, and weaknesses in this can leave organisations extremely vulnerable to attackers. A comprehensive identity scan will look for a host of risks in Active Directory. This will be followed by a detailed report identifying the weaknesses with recommendations for remediating them to help strengthen the company's defences against identity threats and ransomware losses.

* 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: 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.

Threater**

Threater 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.

Darknet Credential Exposure from SpyCloud**

This instant overview of Dark Web data shows a company's risk level and number of times its employees have appeared in breaches. A more detailed report includes those employees' email addresses affected by malware and stolen personal information such as credit card data. All this this can highlight where passwords need strengthening and where more password education is needed.

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.

* 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.

Darknet Credential Exposure from SpyCloud**

This instant overview of Dark Web data shows a company's risk level and number of times its employees have appeared in breaches. A more detailed report includes those employees' email addresses affected by malware and stolen personal information such as credit card data. All this this can highlight where passwords need strengthening and where more password education is needed.

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.

* 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

RESPOND

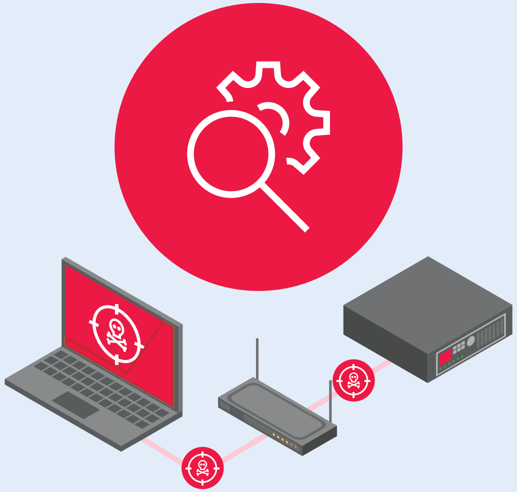
before and after an infection

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:

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.

Incident Response Plan *

CyberEdge clients receive an incident response plan template tailored to their organisation. The template will detail recommended controls to help clients respond effectively to a cyber incident: making it more difficult for attackers and helping the organisation recover quickly from any impacts.

* 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

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

American International Group, Inc. (AIG) is a leading global insurance organization. AIG member companies provide a wide range of property casualty insurance, life insurance, retirement solutions, and other financial services to customers in approximately 70 countries and jurisdictions. These diverse offerings include products and services that help businesses and individuals protect their assets, manage risks and provide for retirement security. AIG common stock is listed on the New York Stock Exchange. Additional information about AIG can be found at www.aig.com | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance www.twitter.com/AIGinsurance | LinkedIn: www.linkedin.com/company/aig. These references with additional information about AIG have been provided as a convenience, and the information contained on such websites is not incorporated by reference herein.

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries and jurisdictions, and coverage is subject to underwriting requirements and actual policy language. Non-insurance products and services may be provided by independent third parties. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insureds are therefore not protected by such funds.

American International Group UK Limited is registered in England: company number 10737370. Registered address: The AIG Building, 58 Fenchurch Street, London EC3M 4AB. American International Group UK Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and Prudential Regulation Authority (FRN number 781109). This information can be checked by visiting the FS Register (www.fca.org.uk/register).

AIG Europe S.A. is an insurance undertaking with R.C.S. Luxembourg number B 218806. AIG Europe S.A. has its head office at 35D Avenue John F. Kennedy, L-1855, Luxembourg. AIG Europe S.A. is authorised by the Luxembourg Ministère des Finances and supervised by the Commissariat aux Assurances, 11 rue Robert Stumper, L-2557 Luxembourg, Grand-Duchy of Luxembourg,
Tel.: (+352) 22 69 11 - 1, caa@caa.lu, www.caa.lu/.