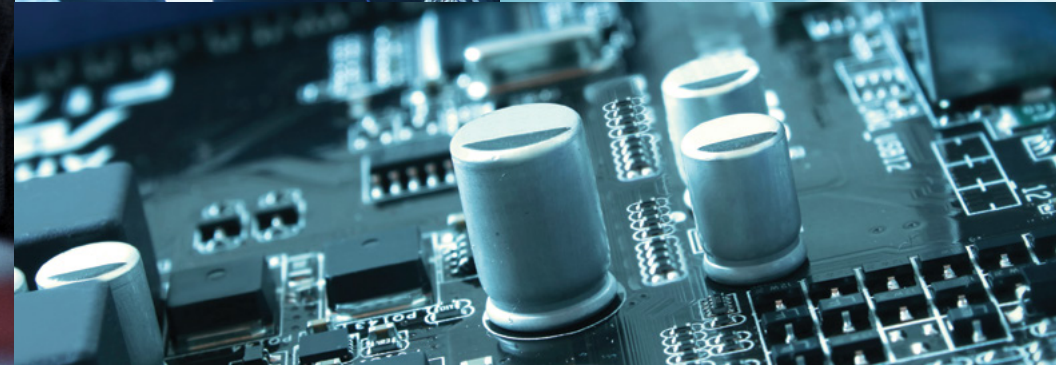


A broker guide to selling cyber insurance



Cyber Sales Playbook



Start >

The Sales Opportunity

Client awareness is soaring

Few lines of business insurance have as many statistics highlighting increasing numbers of incidents and exposures as cyber liability. It is not surprising that so many companies are reported to be thinking about the need for this insurance, while C-Suite and risk managers see cyber exposures as one of their top risk concerns.

Significant impact

While risk managers and executives point to cyber risk as a top concern, cyber exposures are also one of the least insured. This suggests that clients will be very interested in discussing their cyber exposures and possible insurance solutions.

Market opportunity

Organizations have become increasingly concerned about protecting their data, their products, their property, and their reputation. All companies are at risk, presenting brokers with a significant opportunity to assist clients with assessing their exposures and working with carriers to craft solutions.

Cyber is consistently one of the top risks businesses face, with the average cost of a breach at approximately \$3.6 million.¹

Other hot topics:

- Increasing awareness of the potential for reputational harm has led to more C-Suite involvement in strategic cyber initiatives.
- I.T. departments cannot be the sole source for defending against cyber risk.
- Cloud computing and mobile technology are growing areas of concern when it comes to potential sources of cyber risk.
- Clients are increasingly aware of cyber network downtime as a potential loss from a cyber issue.

¹ Ponemon Institute (2017) Cost of Data Breach Study, sponsored by IBM, retrieved from <https://www.ibm.com/security/data-breach>

Target Clients

Any company that relies on technology and stores, manipulates, or transmits data is at risk of a cyber incident.

Manufacturing

Manufacturing and production facilities require integrated, reliable operations systems to ensure their production is timely and effective. Supply chain, outsourcing, and equipment failures are just a few areas that raise the cyber threat risk.

Healthcare

The rise of electronic health records, other digital health platforms, and connected devices have made healthcare more vulnerable to security breaches. According to a recent security threat report, healthcare is becoming one of the most targeted industries.²

Large Business

Many large businesses believe their IT department is effectively managing the risk from cyber threats. This is similar to doctors not carrying malpractice insurance because they have years of medical experience and expertise.

Retail

Retailers hold a wealth of client information including credit and debit card numbers. Clients who typically use the same password and save login details across several accounts are also placed at greater risk for fraud.

Banking/Finance

Financial institutions have long been high on the radar of hackers given the sensitive data at stake. Malware, non-approved devices, and third party business applications all pose unique challenges to banks and other financial companies. **There are approximately 1.2 million new malware or variants on average each day.**²

Small and Mid-sized Business

Mid-sized companies may house large amounts of valuable data – and are more likely to be using legacy systems – but lack the data security budgets of their big business peers. **61% of data breach victims are businesses with under 1,000 employees.**³

Energy

In recent years, increasing attention has been paid to the critical importance of cybersecurity for energy companies. Possible vulnerabilities in industrial control systems and ever greater intersections between operational technology and information technology suggest a significantly heightened exposure, with implications for business interruption, property damage, and bodily injury.

Higher Education

Institutions of higher education are particularly vulnerable to cyber threats due to their open environments, student and faculty information stored, and breadth of services provided. In addition, these institutions may face limited resources and budget constraints, making it difficult for them to keep up with the rapidly changing cyber threat environment.

The experts agree: service providers, financial services, insurance, real estate, and healthcare organizations are the most commonly targeted industries.^{1,2}

See claims scenarios for these industries and businesses >

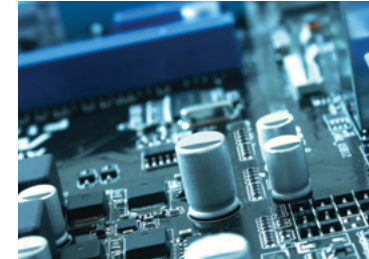
² Symantec (2017) Internet Security Threat Report retrieved from www.symantec.com/security-center

³ Verizon (2017) Data Breach Investigations Report retrieved from <https://www.verizonenterprise.com/verizon-insights-lab/dbir/>

Managing Objections

Most companies today are generally aware of cyber risk. However, some are still uncertain about the exposures they could actually face and others may misunderstand the scope and cost of cyber liability coverage available.

Below are a few suggestions to help manage such objections and overcome these obstacles to purchase.



We already have these measures in place.

Companies may already purchase or deploy certain cybersecurity strategies, but do they know whether or not these services are truly effective? AIG can help assess the current state of your client's cybersecurity posture.

We determine coverage needs based on what our peers are doing.

Every company is unique and cyber criminals, employees, and competitors may be interested in your client's digital assets. AIG has underwritten thousands of cyber policies and has experience across numerous industries. Our underwriting model and corresponding reports can help companies determine their needs through benchmarking and risk reducing controls. [Learn more here >](#)

We weren't aware of the additional services.

Proactive measures to guard against cyber attacks are essential to effective risk management. AIG provides complimentary services such as employee eLearning, blacklist IP blocking, domain protection, and proactive pre-breach consulting to help insureds prevent and prepare for a breach. In addition, our team of experienced cyber risk consultants is available to assist in developing customized risk mitigation strategies through AIG and its partners. Please refer to the [Loss Prevention Services](#) tab of the playbook for additional information.

Our data and/or industry is not a high-risk target for cyber threats.

No company is safe from cyber threats, and bad actors are actively exploiting the vulnerabilities of companies and industries that do not perceive themselves as high risk. Ask your client: could they withstand a complete shutdown of their network for any period of time? There's more than data at stake, and AIG's cyber insurance is there to respond—from network interruption to cyber extortion and optional extensions for third party bodily injury and property damage.

Our IT department is managing risk effectively.

A strong IT department is essential to managing cyber risk; but, given the proliferation of ransomware and daily new variants of malware, it is impossible to prevent every attack. Insurance serves to complement a client's IT department; and, if the worst occurs and their system is breached, it provides the peace of mind of knowing they have a team of experts ready to respond.

The financial cost of an incident would not be significant.

The average cost of a breach is currently estimated at more than \$3.6 million.¹ You may want to look at a breach calculator – like the one in our CyberEdge® mobile app – with your client to estimate costs and assess the potential impact of various scenarios.

Managing Objections Continued

We don't need it. We're not subject to U.S. regulation.

Fines and penalties represent only a portion of the costs that may be incurred as a result of a breach. Organizations must also consider reputational harm, data recovery costs, business interruption, and possible third party liability. In addition, the regulatory environment is constantly evolving, with certain industries adopting standards and best practices separate and apart from government regulation.

Cyber threats are evolving quickly, it is difficult to keep up.

In a rapidly changing landscape, AIG's cyber solutions provide innovative protection and responsive guidance based on years of experience. With AIG's help, businesses keep ahead of the curve when it comes to managing cyber risk.

We don't need it. We aren't a large corporation and don't think our data and/or industry is a high risk for cyber threats.

61% of data breach victims are businesses with under 1,000 employees.³

We don't need it. We outsource our security.

Companies are increasingly moving towards outsourced service providers and cloud-based storage. Still, such providers must be properly vetted. Insureds should read the fine print, as contracts often limit the providers' liability in the event of a breach.

The cost of cyber insurance is too high.

Cyber premiums are modest in comparison to the potential cost of a cyber event, when all components – data recovery, event management, reputational harm, network interruption, and other third party liability – are taken into account. Cyber insurance provides an effective and affordable tool to help manage an incident and mitigate disruption to your client's business.

We don't want to disclose all of our cyber vulnerabilities with you for fear they will be used against us in the event of a claim.

AIG is here to help protect your client's business from a cyber claim. The more information shared, the better we can help protect your client.

Our existing insurance policies typically cover some cyber risk.

AIG offers a comprehensive cyber risk management solution. No other form of liability insurance offers such specialized coverage to assist clients in handling all aspects of a cyber incident. While other policies may offer coverage for certain components of cyber risk, the policy may contain certain exclusions or sub-limits impacting or limiting the coverage.

Cyber insurance can also be packaged with other policies, such as Property Performance Services, to provide additional placement and coverage options.

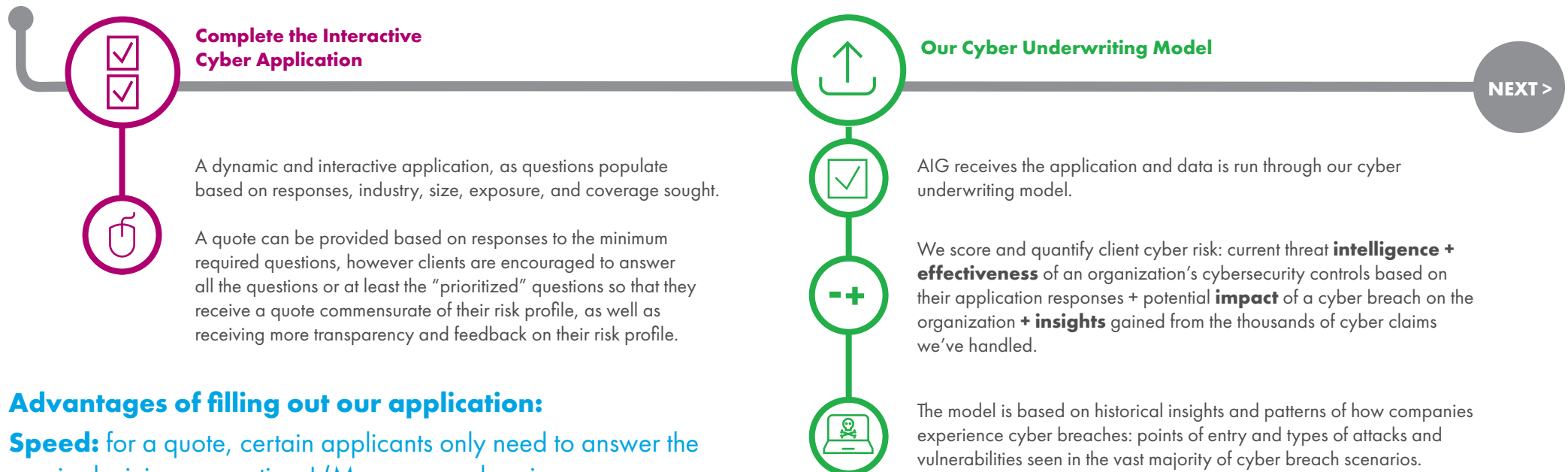
I've never had a cyber breach so I don't need this coverage.

The environment is constantly changing, and with the ever increasing reliance on data, companies may be more susceptible to security and privacy threats than ever before. Future legislation and increasingly stringent industry standards also suggest that the costs of a breach will continue to climb. Proactively managing the risk is crucial.

Client Roadmap

Companies are looking for a way to benchmark their cyber maturity and quantify their cyber exposure. AIG is uniquely positioned to provide relevant feedback, together with actionable insights to assist clients in identifying opportunities to reduce their cyber risk.

Read below to learn how prospective and existing clients can benefit from using AIG's interactive insurance application, cyber underwriting model, and CyberMatics.



Advantages of filling out our application:

Speed: for a quote, certain applicants only need to answer the required minimum questions! (More comprehensive responses may result in a more favourable quote, and with binding, clients receive a detailed risk report, as seen on the next page.)

Personalization: the application is tailored to a client's individual profile and coverage requests/requirements

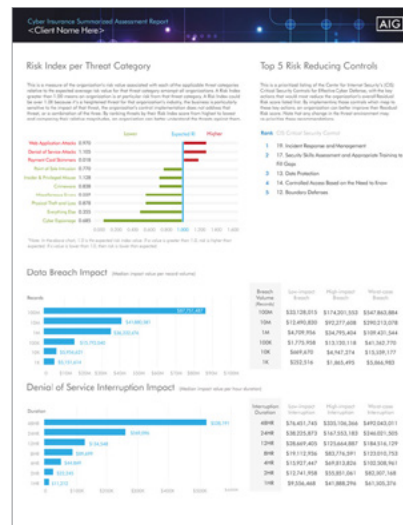
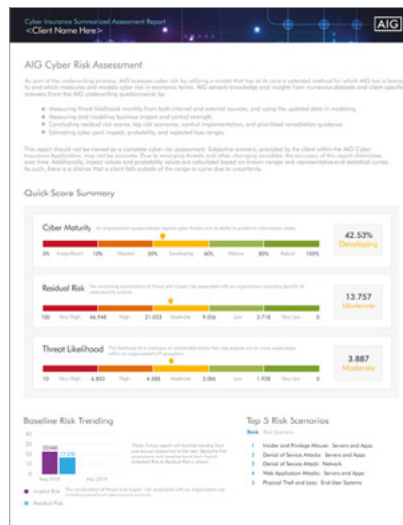
Recognition: comprehensive answers can provide acknowledgment for what clients are doing well

Client Roadmap, cont.

Report generation

< BACK

A sample of a full report with benchmarking and indicators of top risk reducing controls



Cyber Maturity: an organization's preparedness against cyber threats and its ability to protect its information assets

Threat Likelihood: likelihood of a malicious or unintended action that may expose one or more weaknesses within an organization's IT ecosystem

Business Impact: degree of confidentiality, integrity, and availability impact associated with applicable assets within an organization

Control Effectiveness: indicates how much each control reduces risk, depending on how well the controls are implemented

Implicit Risk: combination of threat and impact risk associated with an organization, not including benefits of cybersecurity controls

Residual Risk: remaining combination of threat and impact risk associated with an organization, including benefits of cybersecurity controls

Applicants who submit the new application can receive a basic level report, even if they do not bind their cyber insurance with AIG.

Insureds who submit the new application and bind coverage with AIG receive a full report with benchmarking information, when available.
The full report can help clients indicate top risk reducing controls.

Why is this useful?

CISOs can use this information to understand their organization's threat profile and resilience in detail, by both attack type and asset class, and further use the model's mapping on how different controls affect each risk scenario to adjust the overall security maturity of an organization.

Enhancing the cyber underwriting model, CyberMatics™, AIG's patent pending security services-led approach, provides AIG with a more accurate and up-to-date risk assessment of a client's IT environment, and provides the building blocks to offer insights directly to the client on a real time basis.

Proactive loss prevention services to further improve a client's cyber maturity >>

Proactive Loss Prevention Services

Optimizing the value of CyberEdge

Do insureds understand the suite of services potentially available beyond the insurance policy? AIG supports an end to end risk management approach, with numerous breach prevention and risk consultation services.

Complimentary Tools and Services

Complimentary tools and services are included with many cyber policies* to provide knowledge, training, security, and consultative solutions. Services include employee cybersecurity eLearning; blacklist IP blocking; domain protection; legal, forensic, and PR consulting; and more.

[LEARN MORE >](#)

AIG Services

AIG's team of cyber risk consultants brings over 50 years combined experience in IT security to help our clients stay ahead of their cyber risk. Our team works directly with insureds to provide detailed, technical expertise and consulting services to improve their cyber maturity.

[LEARN MORE >](#)

Trusted Vendor Partners

We have partnered with experts in cyber risk to bring our clients additional options to add to their line of defence.

[LEARN MORE >](#)

CyberMatics™

With CyberMatics, our patent-pending security services-led approach, we can provide significantly more insightful and tailored analytics that, when blended with risk consulting, can improve the risk profile of our clients.

[LEARN MORE >](#)

Proactive Loss Prevention Services

Complimentary Tools and Services

Complimentary tools and services are included with many cyber policies* to provide knowledge, training, security, and consultative solutions.

Employee Cybersecurity eLearning – Available in 11 languages

Meaningful, sustainable, and measurable cyber risk reduction eLearning to reference and reinforce clients' security policies based on employees' individual roles.

Blacklist IP Blocking and Domain Protection – Reduces the attack surface up to 90% ahead of the firewall

Enables organizations to control their exposure to criminal activity by leveraging vast threat intelligence repositories, precision geo-blocking, and black-list automation to reduce risk.

Infrastructure Vulnerability Scan – Identification of high risk infrastructure vulnerabilities

Select parts of your internet-facing infrastructure to have experts examine and identify vulnerabilities that are open to potential exploits by cyber criminals.

Legal Risk Consultation – Review and strengthen incident response capabilities

Two hours with an expert on incident response planning, regulatory compliance, security awareness, or privacy training.

Forensic Risk Consultation – Organizational preparedness for different threat scenarios

One hour with a forensic expert on what an organization needs to think about and prepare for different threat scenarios.

[COMPLIMENTARY TOOLS AND SERVICES >](#)[TRUSTED VENDOR PARTNERS >](#)[AIG SERVICES >](#)[CYBERMATICS >](#)

Public Relations Risk Consultation – Crisis communication plan best practices and preparation

One hour with an expert to prepare and plan for your organization to handle potential scenarios if one should occur.

CyberEdge Hotline – 24/7/365 cyber hotline

Our CyberEdge Claims Hotline is available 24/7/365 at 1-800-CYBR-345 (1-800-292-7345). Once a call is made, the CyberEdge 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 (such as a hacker inside a network), and start the restoration and recovery processes.

Insurance Portfolio Diagnostic – Cyber as a peril analysis against insurance portfolio

Experts review your entire property and casualty portfolio to determine how it is anticipated to respond to the spectrum of cyber predicated financial and tangible losses.

Cybersecurity Information Portal – Online access to cybersecurity information

24/7/365 access to current cybersecurity information.

Visit www.aig.com/cyberriskconsulting to request more information on these services.

Compare AIG's complimentary risk consulting and loss prevention services to other carriers' [CLICK HERE](#)

*Clients who purchase CyberEdge and spend more than \$5,000 in premium qualify for the above services.

The tools and services described above may be modified (by adding, removing, or replacing a tool or service) or discontinued at any time.

Proactive Loss Prevention Services

AIG Risk Consulting Services

AIG's team of cyber risk consultants brings over 50 years combined experience in IT security to help our clients stay ahead of their cyber risk. Our team works directly with insureds to provide detailed, technical expertise and consulting services through:

Cyber Defence Review, designed to take a look at an insured's people, processes, and tools comprising their cybersecurity program and identify strengths and weaknesses. [Learn more >](#)

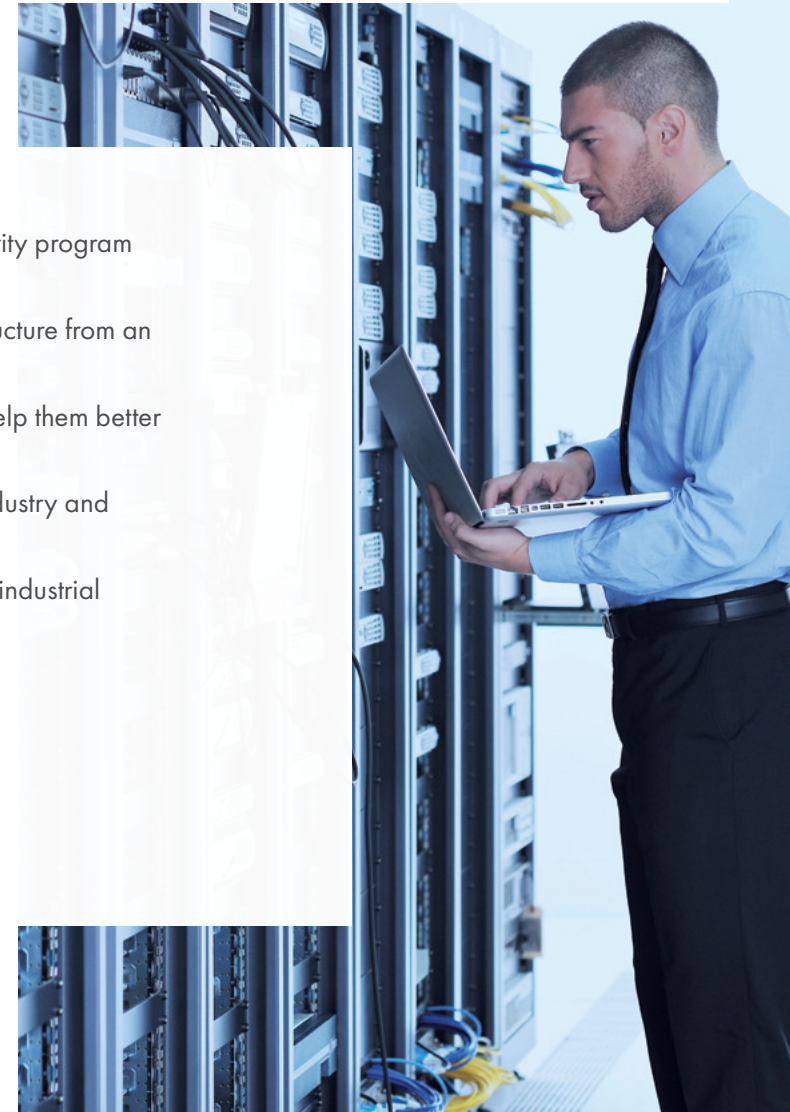
Internet-Facing System Examination, designed to help insureds identify risks and exposures in their public facing infrastructure from an attacker's perspective. [Learn more >](#)

Incident Simulation Workshop, designed to help clients ensure their incident response plan will respond efficiently and help them better maximize their CyberEdge benefits. [Learn more >](#)

Executive Threat Brief, designed to help clients better understand the current security threat landscape specific to their industry and current methods attackers are using. [Learn more >](#)

Cyber Engineering Study, designed to look at an insured's people, processes, and tools that protect critical systems and industrial controls within their environment. [Learn more >](#)

For more information on CyberEdge's loss prevention and risk consultation services, email us at CyberRiskConsulting@aig.com.

[COMPLIMENTARY TOOLS AND SERVICES >](#)[TRUSTED VENDOR PARTNERS >](#)[AIG SERVICES >](#)[CYBERMATICS >](#)

Proactive Loss Prevention Services

Preferred Vendor Partner Services

We have collaborated with experts in cyber risk to bring our clients additional options to add to their line of defense. All CyberEdge clients have access to the following services at a preferred rate, some of which are available for a free demo.

Quantification Workshop and Insurance Portfolio Stress Test, powered by AXIO, helps clients understand their cyber exposure in financial terms and subsequently, how a variety of representative cyber loss scenarios might be treated by the client's entire insurance portfolio.

BitSight Security Ratings, powered by BitSight Technologies, and **Vendor Security Ratings**, powered by SecurityScorecard, let companies measure and monitor their own network and those of their third-party vendors.

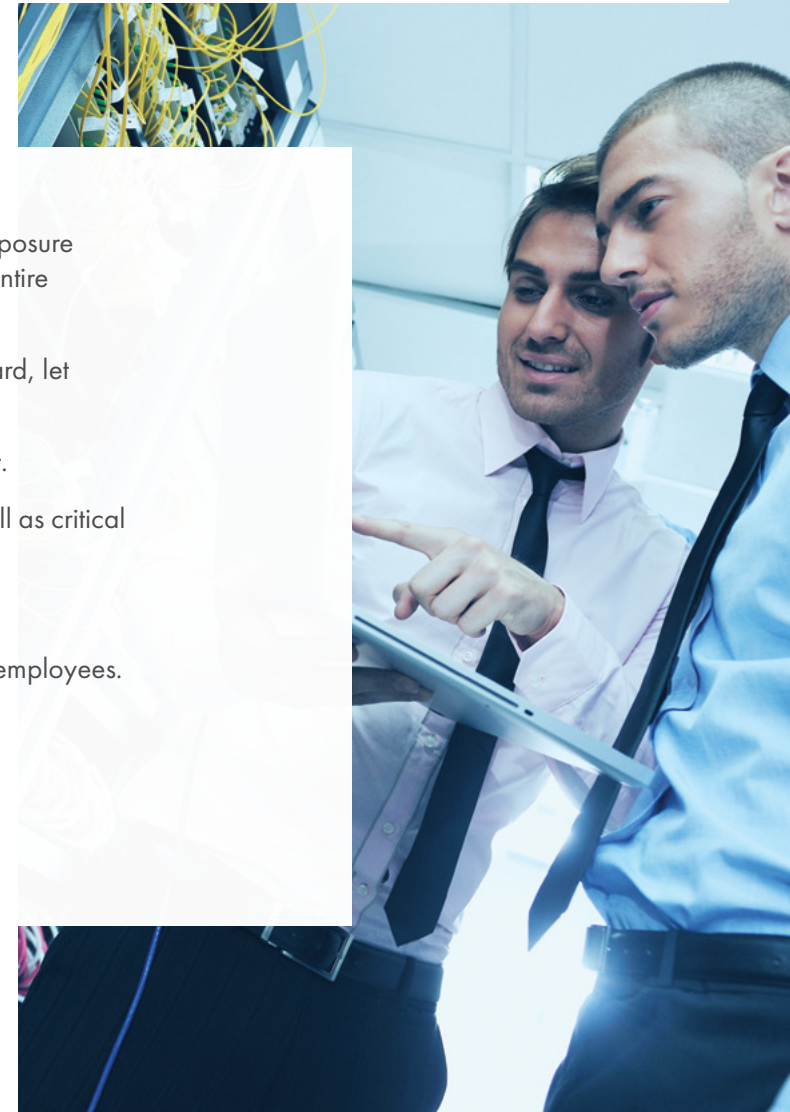
Dark Net Intelligence, powered by BlueVoyant, helps clients stay apprised of what the latest chatter is inside the dark net.

Office of the CISO, powered by Optiv, provides on-demand access to virtual, interim, and staffed CISO expertise as well as critical security advisory services.

Cybersecurity Maturity Assessment, powered by RSA, helps organizations assess their cybersecurity risk.

Security Awareness Training, powered by Wombat Security, provides phishing training and simulations for an insured's employees.

For more information on CyberEdge's loss prevention and risk consultation services, email us at **CyberRiskConsulting@aig.com**.

[COMPLIMENTARY TOOLS AND SERVICES >](#)[TRUSTED VENDOR PARTNERS >](#)[AIG SERVICES >](#)[CYBERMATICS >](#)

Proactive Loss Prevention Services

CyberMatics™

AIG can provide significantly more insightful and tailored analytics that can improve the risk profile of our clients.

Our ability to provide these insights was previously limited due to the lack of verifiable data and visibility into the client's network.

Our solution? Obtain verified data from the client's network and map it to our application question set to feed our Cyber Underwriting Model, enabling us to provide timelier cyber risk solutions than ever before –

We call this CyberMatics.

New underwriting application process

+

= Improved Client Risk Score

Verified client data received from
DarkTrace or CrowdStrike

- Only clients using CrowdStrike or DarkTrace are currently eligible for CyberMatics.
- Once a client signs up for CyberMatics, it will need to give CrowdStrike and Darktrace permission to share verified data relevant to the cyber underwriting model with AIG.
- The vendor will pull the information from the client's network regularly, translate the information into data relevant to the cyber underwriting model, and provide the data to AIG.

[COMPLIMENTARY TOOLS AND SERVICES >](#)
[TRUSTED VENDOR PARTNERS >](#)
[AIG SERVICES >](#)
[CYBERMATICS >](#)


Darktrace is the world's leading machine learning company for cyber security. Created by mathematicians from the University of Cambridge, the Enterprise Immune System uses AI algorithms to automatically detect and take action against cyber-threats within all types of networks, including physical, cloud and virtualized networks, as well as IoT and industrial control systems. A self-configuring platform, Darktrace requires no prior set-up, identifying advanced threats in real time, including zero-days, insiders and stealthy, silent attackers. Headquartered in San Francisco and Cambridge, UK, Darktrace has 30 offices worldwide.



CrowdStrike is the leader in cloud-delivered endpoint protection. Leveraging artificial intelligence (AI), the CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. CrowdStrike Falcon deploys in minutes to deliver actionable intelligence and real-time protection from Day One. It seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by 24/7 managed hunting. Its cloud infrastructure and single-agent architecture take away complexity and add scalability, manageability, and speed.

AIG Cyber Coverage

(Note that this is only a summary for general guidance and scope; actual coverage is subject to the terms and conditions of the policy.)

Cyber is a peril that may cause loss in both the physical and non-physical world. AIG's Cyber solutions help protect clients across the spectrum of cyber risk.

- **CyberEdge®** covers the financial costs associated with a breach, including event management, data restoration, financial costs to third parties, network interruption, and cyber extortion.
- **CyberEdge Plus** covers losses in the physical world caused by a cyber event, including primary coverage for business interruption, first and third party property damage, physical injury to third parties, and products/completed operations coverage. [Learn more.](#)
- **CyberEdge PC®** sits excess of traditional property and casualty policies on a DIC/DIL basis.
- **Property Performance Series** can be broadened to include electronic data loss or network business interruption
- **WorldRisk Foreign Package** policies with General Liability coverage can be enhanced with Security and Privacy Liability Insurance and Event Management Insurance.
- **CrisiSolution®**, AIG's Kidnap, Ransom & Extortion policy, can be enhanced with Cyber Extortion Incident Response and Business Interruption coverage

See our [Cyber Cover Grid](#) for guidance on choosing the right purchasing channel for your client.

Financial losses

Third party loss resulting from a security or data breach

Defence costs and damages if the business (or its outsourced handling firm) causes a breach of personal or corporate data

Defence costs and damages if the business contaminates someone else's data with a virus

Defence costs and damages if the business suffers theft of a system access code by non-electronic means

Event management costs

Costs of notification, public relations, and other services to manage/mitigate a cyber incident

Expenses to restore, recreate, or recollect lost electronic data

Forensic investigations, legal consultations, and identity monitoring costs for breach victims

Expanded network interruption

Loss of net profit and extra expense as a result of a material interruption to the insured's network caused by a security breach

Expanded cyber/privacy extortion

Ransom payments (extortion loss) to third parties incurred in terminating a security or privacy threat

Expanded digital media liability

Damages and defence costs incurred in connection with a breach of third party intellectual property or negligence in connection with electronic content

Tangible losses (physical losses)

Expanded business interruption

Covers business income loss and expenses to reduce loss as a result of a breach involving property damage

First party property damage

Covers physical loss or damage to insured property as a result of a breach

Third party bodily injury and property damage

Covers bodily injury or damage to others' property caused by a breach

Products/Completed Operations Coverage

Covers bodily injury or property damage caused by a breach of a computer system that is part of an insured's product

[NEXT CYBER COVERAGE PAGE >](#)

AIG Cyber Coverage

Channels to Purchase Coverage

Cyber Coverage Channels

Click on product names to learn more

	CyberEdge®	CyberEdge Plus	Property Performance	CrisiSolution®	WorldRisk Foreign Commercial Insurance	CyberEdge PC®
Third party claims arising out of, or alleging financial loss as a result of a failure of the insured's network security or a failure to protect confidential information	✓				✓	Excess-Difference in Conditions solution to enhance and fill gaps in coverage for cybersecurity risk
Investigation and defence of regulatory actions arising out of a failure of the insured's network security or a failure to protect confidential information, including coverage for such fines and penalties if allowable by law	✓				✓	
PCI-DSS (Payment Card Industry Data Security Standard) assessments for the failure to protect payment card data	✓				✓	
Costs of notifications, public relations, and other services to assist in managing and mitigating a cyber incident; legal consultations and identity monitoring costs for victims of a breach are included	✓				✓	
Forensic investigation costs due a covered cyber event	✓		✓	✓	✓	
Costs to restore electronic data from duplicates or, if not possible, costs to research, gather, and assemble electronic data due to a covered cyber event	✓		✓			
Responds to a material interruption of an insured's business operations providing for business interruption and certain expenses due to a covered cyber event	✓		✓	✓		
Reimbursement of ransom payments incurred in terminating a covered cyber event	✓			✓		
Business income loss resulting from physical damage to property due to a covered cyber event		✓	✓			
Loss associated with first party property damage due to a covered cyber event		✓	✓			
Third party claims alleging bodily injury or third party property damage caused by a security failure or privacy event		✓				
Third party claims alleging bodily injury and third party property damage caused by a breach of a computer system that is part of an insured's product		✓				
Coverage Form	Specialty Risk Protector		Standalone policy form	Endorsement to CrisiSolution policy	Endorsement to WorldRisk CGL policies	Standalone policy form

What constitutes a "covered cyber event" may vary by type of coverage and policy form, and all statements are subject to the terms, conditions, and exclusions of the specific policy.

Global Claims Expertise

AIG's Cyber claims team is ready to assist clients as soon as they suspect a potential network breach. Our team has local presence supported by global resources, allowing our experts to manage unfolding events and quickly respond to inquiries. We help clients notify and support the recovery of affected customers, handle crisis communications, and determine exactly what happened.

We process approximately four cyber claims every business day, giving us the insight and expertise to understand complex cyber incidents. Our underwriting and claims teams partner to help create the best possible experience and avoid any miscommunication from the beginning to end of the process.

Claims Benefits

- 24/7 access to our claims team to report a claim or seek guidance
- Access to local claims specialists and panels of domestic and international legal advisors on the ground around the world with the local expertise to handle cyber claims
- Complimentary one hour consultation with breach counsel and access to a breach response team to prepare for a cyber attack

Unprecedented Experience

Our claims specialists are ready to help policyholders manage a cyber incident from the moment it occurs. Our team provides the additional layer of defence an IT department needs to face the issue and its consequences.

Rapid Support When Clients Need it Most

- Our claims specialists react quickly to guide our clients, from assessing their needs to processing their claim.
- Most coverage is written on a primary basis, enabling our claims specialists to be on the front line with the authority to make decisions.
- Our network of legal firms, forensic investigators, and public relations firms offer immediate support for insureds managing the consequences of a breach.

Rapid Technical Support

- Our Cyber Claims Hotline is available 24/7. Once a call is made, the claims team will coordinate with the client to implement their response plan, engage any necessary vendors including breach counsel and forensics firms to identify immediate threats (such as a hacker inside a network), and start the restoration and recovery processes.

Add our expertise to yours

AIG provides breach coaching, forensic services, and insurance to get your client's business back to normal after a cyber event.

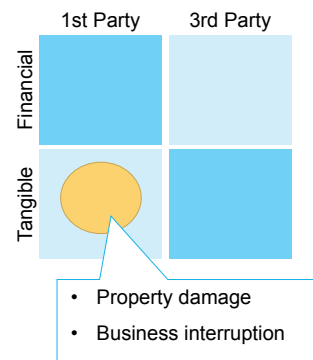
After calling the AIG Cyber Claims Hotline, clients may expect:


[CLAIMS SCENARIOS >](#)

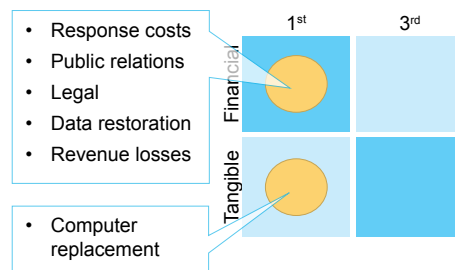
Cyber as a Peril Scenarios

Property Damage & Business Interruption

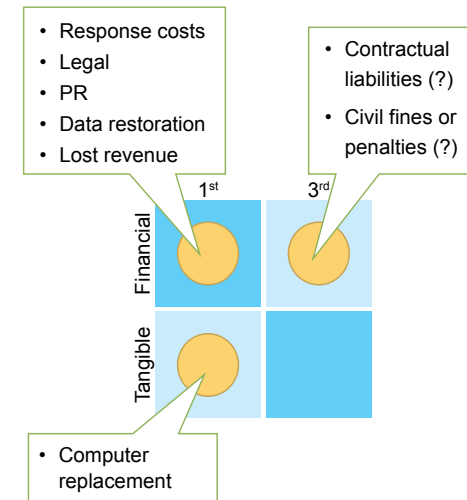
Destructive cyber attack against a European manufacturer: Hackers manipulated the manufacturer's control system, preventing its blast furnace from shutting down, and causing significant property damage.



Cyber attack against a large energy company: Malware deployed by an insider with privileged access destroyed data and rendered 30,000 computers inoperable.

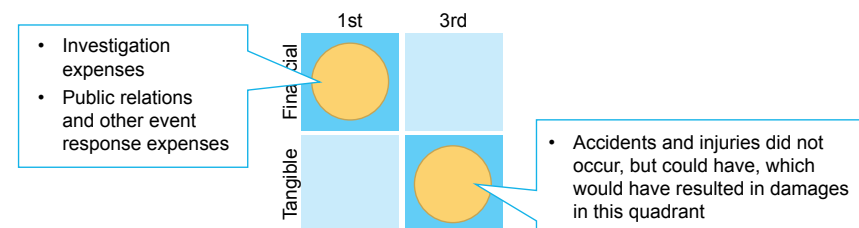


Coordinated attack against an electric utility: Long term reconnaissance and multiple coordinated efforts involving spear phishing emails, malware, harvested credentials, and flooded call centres enabled attackers to manipulate the electric utility's SCADA system, causing a power outage for hundreds of thousands of customers.



Bodily Injury and Products/Completed Operations Coverage

Demonstrated ability to hack vehicles of a major auto manufacturer: White hat hackers demonstrated their ability to remotely take control of a vehicle—no injuries resulted, but it demonstrated the potential for a cyber attack against products linked to the internet.



Claims Narratives by Industries

AIG has helped more than 22,000 companies face a cyber attack, uniquely positioning us to identify and anticipate claim trends and settlement values. Following are a range of scenarios that demonstrate AIG's cyber claims expertise in action.

Healthcare

Healthcare - Data Theft

An insured hospital was notified of a potential breach involving protected health information (PHI) of over 40,000 patients.

AIG quickly engaged with the insured to retain breach counsel and the further retention of a forensic investigator. Based on the ensuing investigation, we coordinated with the insured and breach counsel on the selection and retention of vendors to handle the required notification to regulators and patients, offered patients access to identity monitoring protection, and established a call centre to handle inquiries and registration for the identity monitoring protection. AIG reimbursed the insured \$450,000 for

Credit Monitoring and ID Theft Insurance; \$175,000 in notification and call centre costs; \$25,000 in forensic costs; and \$90,000 in legal costs. The policy also covered \$500,000 in regulatory fines assessed on the insured.

Data Theft

A physician's email account was hacked and all his email was automatically forwarded to an email account in Eastern Europe – jeopardizing personal information of more than 3,500 patients.

AIG's quick response and vendor relationships helped the insured quickly retain experts to guide the organization through all steps required to effectively handle the breach: notification, establishment of a call centre, and bringing in the regulatory body.

Rogue Employee

An office employee stole the medical profiles and histories and detailed personal identity information of approximately 125,000 patients of an insured hospital.

AIG and the insured collaborated to form a crisis support team of outside professionals and reimbursed the hospital approximately \$800,000 for expenses associated with this crisis team. Subsequently, AIG helped the insured work through a second breach using experienced vendors from our expansive cyber security network.

Financial Institutions

Data Theft

An email server and external hard drive of our client were stolen from the premises of an outside vendor. Personal information of approximately 175,000 individuals was compromised.

AIG worked closely with the insured and provided reimbursement of \$1 million for notification and the retention of professionals.

Malware

Hackers gained entry to an insured's point of sale system and, before they were detected, were able to access over five million customer credit and debit card numbers.

AIG quickly engaged with the insured to retain breach counsel and the further retention of a forensic investigator and a payment card industry (PCI) forensic investigator. Based on the ensuing investigation, we coordinated with the insured and breach counsel on the selection and retention of vendors to manage the public relations messaging and the necessary notification to regulators and consumers, offered consumers access to credit

monitoring protection, and established a call centre to handle inquiries and registration for the credit monitoring protection. Breach counsel was utilized to handle the defence of a dozen class action lawsuits and Federal and State regulatory investigations. The CyberEdge policy provided coverage for this activity, including event management expenses of \$750,000 for forensics, \$3 million for the credit monitoring, notification, and call centre, and \$50,000 for public relations. The CyberEdge policy provided further coverage of \$1.5 million for breach counsel, \$1.2 million in regulatory fines, and \$2 million in PCI fines.

Claims Narratives by Industries Continued

Higher Education

Security Breach

A university audit uncovered a security breach which allowed unauthorized individuals to access the financial aid roster, including personal data.

AIG's cyber security specialists assisted the university in conducting a forensic audit, which determined that more than 18,000 student records may have been compromised. AIG also helped the university select vendors to provide call centre services and credit monitoring. AIG reimbursed the insured approximately \$70,000 above the retention for the vendors' services.

Credit Card Theft

Three credit card pay station machines were compromised at a large university, and the university's IT department discovered a breach shortly thereafter in the university's network stemming from the pay station incident.

AIG's cyber security specialists stepped in quickly to assist in the investigation. AIG worked with the insured to retain a forensic auditor as well as a breach coach and is evaluating the need for credit-monitoring services.

Corporate Data Risk

A college inadvertently sent an email to approximately 80 students that attached a file containing personal data for all of its students. Working together, AIG and the college were able to retrieve 55 of the emails before they were opened. AIG worked closely with the school's dean of students and arranged notification and credit monitoring for the impacted students.

Identity Theft

A laptop containing a database with personally identifiable information numbers of nearly 7,500 current and former university students was stolen, along with the password for the data on the hard drive. Several students reported that third parties attempted to activate credit cards in their names. AIG added its expertise to the university's with immediate assistance including call centre services, an anti-fraud protection vendor, credit-monitoring services, and counsel. AIG's quick response enabled the university to provide students with timely services to mitigate the risk of identity theft.

Lawyers/Healthcare

Stolen Property

A laptop and briefcase belonging to the insured's general counsel were stolen from his car. Included in the theft was a folder containing billing audits including birth dates of more than 200 hospital patients.

AIG and the insured determined sufficient confidential information had been compromised to warrant notification. AIG retained counsel to act as a breach coach for the insured and provided those affected with a year of credit-monitoring services. To date, no third party claim has been made.

Business Interruption

An associate who had resigned from an insured law firm erased all accessible hard drives and removed the firm's intellectual property and primary information from back-up systems.

AIG's experienced cyber security response team worked closely with the firm to recreate all of the applications and information that had been erased and reimbursed the insured for an estimated \$300,000 in costs.

Manufacturing

Ex-Employee Hacking

Following the termination of his job at a paper manufacturer, a former employee realized he could still access company services via virtual private network (VPN). Once in the company network he installed software to manipulate the industrial control systems and caused over \$1 million in lost production.

Ransomware

An automotive manufacturer was forced to halt production at one of its manufacturing plants when it discovered a ransomware virus had infected its computer network. Production at the plant completely halted.

Forced System Failure

A global computer outage affected a medical device manufacturer's ability to produce goods and fulfill orders for multiple days. Employees were brought in for overtime hours to ensure orders were fulfilled in the timeliest manner possible.

Claims Narratives by Industries Continued

Retail

Malware

A pub was notified by a credit card company of a potential account data compromise.

On behalf of the pub's payment processor, AIG helped the merchant retain a forensic investigator who found that malware had been installed on its server. AIG called on its extensive cyber security expertise and worked with the merchant's payment processor to help replace the compromised server and fortify its data security. On behalf of the payment processor, AIG reimbursed the merchant \$17,000 for the audit-related services.

Corporate Data Risk

A luxury department store chain learned of a potential incident involving an unknown credit card processor that put personal information for more than 35,000 store cardholders at risk.

Calling on its strong vendor relationship network, AIG worked with the insured to retain top professionals to provide notification, replacement credit cards, and credit-monitoring services. AIG reimbursed the insured approximately \$200,000. AIG is providing legal counsel and closely collaborating with the retailer to explore its right to reimbursement from the credit card company and third party processor.

Security Breach

Approximately three million passwords were stolen from an insured online service provider and leaked on the internet.

AIG's claims team and breach coach worked closely with the insured in recommending that affected individuals reset affected passwords, recommending security tips for users, emailing three million potentially impacted customers, and providing information on how to contact the insured's customers care team.

Identity Theft

An insured car dealership was notified of the theft of a box containing sales files and, after investigation, determined that additional boxes containing sales contracts with personal customer information were also missing.

Although the applicable notification law did not apply because the files were in paper format, AIG urged the insured – and they agreed – to provide voluntary notification to potentially affected customers. AIG also retained a breach coach to assist the insured and provided free credit monitoring for one year to affected individuals.

Network Interruption

Hackers accessed the insured's system through a targeted spear-phishing attack. The hackers placed ransomware on the system, which once activated encrypted all the data on the insured's systems. Seven servers and hundreds of PCs were affected. The hackers demanded 12 Bitcoin for the encryption keys. The insured engaged with AIG's cyber claims specialists to coordinate the retention of breach privacy counsel and a forensics firm to respond to the event. AIG and breach counsel coordinated efforts with law enforcement. The insured and the forensics firm were unable to unencrypt the insured's data and, after consultation with AIG and law enforcement, the insured made the decision to pay the ransom.

We facilitated the retention of vendors to procure the necessary Bitcoin for payment of the ransom. Once paid, the insured received the necessary encryption keys. The systems were then gradually brought back online over the course of several days. Ultimately the insured's business systems were offline for 2.5 business days. AIG reimbursed the insured \$4,500 for the ransom, \$2,500 in Bitcoin procurement expenses and payment, \$950,000 in forensic investigation and remediation, \$65,000 in legal costs, and \$32,000 in public relations costs. In addition, AIG reimbursed the insured \$1.1 million for its lost income and \$850,000 for additional expenses associated with the outage.

Credit Card Theft

The IT manager of an auto parts business discovered that a file which was not part of the company's website was being used to steal payment card information.

On behalf of the insured's payment processor, AIG assisted the merchant in retaining a forensic auditor and reimbursed \$7,000 for the forensic audit and \$3,500 for credit card company fees and fines.

Suspected Breach

A credit card company notified a pharmacy of a suspected breach.

The merchant was required by the credit card company to conduct a forensic investigation to ensure that its payment-processing environment was compliant with PCI-DSS.

Putting its extensive experience in cyber security to work, AIG, on behalf of the merchant's payment processor, helped conduct a forensic audit which demonstrated that the merchant was compliant.

Claims Narratives by Industries Continued

Cyber Extortion

Malware was placed on the network of a law firm when an employee fell victim to a phishing scheme. The malware was downloaded when the employee opened what appeared to be a valid video conference invitation. The extortionist threatened to shut down the system and prevented the insured from accessing its data unless the insured paid 10 Bitcoin. The extortionist indicated that the demand would increase each week until payment was made.

AIG quickly engaged with the insured to retain breach counsel and the further retention of a forensic investigator. Breach counsel and the insured reported the matter to the FBI. The forensic investigation determined that the extortionist had the capability to fulfill the threatened action and confirmed that the insured did not have a reliable back up source for its data. The CyberEdge policy provided coverage for the ransom payment as well as \$25,000 for breach counsel and \$85,000 for the forensic investigator to assess the threat and to ensure that the malware was eradicated.

Cyber Extortion

An insured's computer server was maliciously attacked by a virus that encrypted their data and demanded a \$5,000 ransom to un-encrypt. The insured reported the matter to law enforcement and local authorities. The insured did not pay the ransom on the advice of the law enforcement; rather AIG worked with the insured to engage an expert to perform a forensic analysis of their system. The forensic expert was able to determine that the impacted server did not contain any confidential information but rather the company's warehouse inventory information.

The forensic expert was able to remove the virus and strengthen the insured's data security protections. AIG reimbursed the insured more than \$45,000 for forensic costs incurred.

AIG Cyber Contacts:

Head of Cyber, U.S. & Canada	Greg Vernaci	greg.vernaci@aig.com	212-458-2518
Manager, Cyber and Professional Liability Financial Lines	Ruby Rai	ruby.raai@aig.com	416-596-3920
Head of Client Risk Consulting	Phil Kibler	philip.kibler@aig.com	317-967-3927
Risk Consultant	Razmik Ghanaghounian	razmik.ghanaghounian@aig.com	416-646-3782
Claims	Joe Fidilio	joe.fidilio@aig.com	416-596-4010

For more information, contact your underwriter or email us at CyberEdge@aig.com.

www.aig.ca



American International Group, Inc. (AIG) is a leading global insurance organization. Founded in 1919, today AIG member companies provide a wide range of property casualty insurance, life insurance, retirement products, and other financial services to customers in more than 80 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 and the Tokyo Stock Exchange.

Additional information about AIG can be found at www.aig.com and www.aig.com/strategyupdate | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance | LinkedIn: <http://www.linkedin.com/company/aig>.

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. AIG Insurance Company of Canada is the licensed underwriter of AIG Commercial and Consumer insurance products in Canada. Coverage may not be available in all provinces and territories and is subject to actual policy language. Non-insurance products and services may be provided by independent third parties. The AIG logo and AIG are trademarks of American International Group, Inc., used under license by AIG Insurance Company of Canada. Additional information about AIG Canada can be found at www.aig.ca.

© 2018 American International Group, Inc. All rights reserved.