THE POTENTIAL THAT DIGITALIZATION ENTAILS IS ENORMOUS AND ITS FULL SCALE CAN HARDLY BE ASSESSED. HOWEVER, ...

Time and again, we have seen how vulnerable digital progress has made us. “Petya” and “WannaCry” have also proven this point. Companies of all sizes were affected – the consequences included business interruptions and significant costs for the restoration of IT systems.

The new laws on data security also pose challenges of their own. The Data Protection Regulation of May 28, 2018 provides for, amongst other things, stricter reporting obligations with regard to cyber incidents (72 hours) and a “right to be forgotten” in respect of customer data. In the future, breaches will lead to significantly greater sanctions, including administrative fines of up to 4% of global revenue or EUR 20 million.

The fact that the threat posed by cyber incidents is being taken ever more seriously by the industry is also reflected in the Allianz Risk Barometer. In 2018, cyber risks, both worldwide and in Germany, ranked second on the risk scale.

However, every company can take measures to counter this threat: risk management in line with the company’s own threat level, cooperation with specialists from the outset, and insurance to protect against purely financial losses.

This sort of all-encompassing solution is offered by Allianz Cyber Protect Premium. This product exceeds the benefits provided by conventional insurance policies. Not only does it cover losses resulting from cyber incidents; it also provides access to a select network of experts: specialists who support and assist the insured prior to, during and after a loss event.
ASSESS:
Individual risks and threat scenarios are identified in all departments; a common understanding of one’s own business model, value chain, the IT “crown jewels” is required.

PREVENT + PROTECT:
Making your own IT security resilient – investing in your technology, creating crisis plans for cyber incidents, and conducting crisis exercises. Protecting against any remaining risks via insurances.

DETECT:
IT is subject to constant monitoring with regard to anomalies, e.g. with the aid of early-warning tools; information and ideas with regard to external threats are exchanged internally and across company borders.

RESPOND:
Using expert know-how in the event of cyber incidents: forensic services for the assessment of loss, crisis management, legal advice or PR consultancy. All this contributes towards taking the right measures – in order to, for example, appraise the incident for use in court – and towards preventing similar incidents in the future.

### EVALUATION RESULTS OF CYBER LOSSES REPORTED TO AGCS - 2013-2017

For every 10 cyber-policies taken out, 1 loss event is reported – mostly a combination of first-party and third-party damage.

Business interruptions as well as data breaches incur the highest expenses.

Services due to data breaches and Forensics services are most frequently made use of.

### FROM PRECAUTIONARY MEASURES TO CRISIS MANAGEMENT – HOW COMPANIES (SHOULD) COUNTER THEIR CYBER RISKS

<table>
<thead>
<tr>
<th>AVERAGE LOSS</th>
<th>HIGH</th>
<th>MEDIUM</th>
<th>LOW</th>
<th>RARE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber BI (after Cyber attack, human error or technical failure)</td>
<td>Data Privacy breach (incl. Data breach response costs &amp; notification costs)</td>
<td>Cyber Crime / Hacker Theft</td>
<td>E-Payment / PCI General 3rd party liability (after Cyber incident)</td>
<td>Forensics Services</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CLAIMS FREQUENCY</th>
</tr>
</thead>
<tbody>
<tr>
<td>RARE</td>
</tr>
</tbody>
</table>

### CYBER LOSSES SPEAK FOR THEMSELVES …

<table>
<thead>
<tr>
<th>CYBER BI (after Cyber attack, human error or technical failure)</th>
<th>Data Privacy breach (incl. Data breach response costs &amp; notification costs)</th>
<th>Cyber Crime / Hacker Theft</th>
<th>E-Payment / PCI General 3rd party liability (after Cyber incident)</th>
<th>Forensics Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIGH</td>
<td>Data Privacy breach (incl. Data breach response costs &amp; notification costs)</td>
<td>Cyber Crime / Hacker Theft</td>
<td>E-Payment / PCI General 3rd party liability (after Cyber incident)</td>
<td>Forensics Services</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>Data Confidentiality breach</td>
<td>Cyber Extortion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LOW</td>
<td>Data Confidentiality breach</td>
<td>Cyber Extortion</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| RARE | MEDIUM | FREQUENT |
|----------------|
| RARE | MEDIUM | FREQUENT |
THE SOLUTION: ALLIANZ CYBER PROTECT

Insurance coverage

OWN DAMAGE
• costs of crisis management
• costs for communication
• business interruption – also for human error or technical problems (period of indemnity – 180 days) and restoration
• cyber theft
• physical loss or damage to IT hardware
• betterment costs

COVER IS ALSO PROVIDED FOR
• prevention of cyber crises
• the payment of legally permissible administrative fines
• losses as a consequence of cyber extortion
• costs in connection with official data protection proceedings

FOR LIABILITY CLAIMS
• confidentiality and data breaches
• breaches in network security
• digital communication
• e-payment/contractual penalty

INSURANCE COVER FOR INITIAL RESPONSE (without deductible for the first 48 hours following call to the AGCS Cyber Emergency Hotline)

Services rendered by external specialists for all phases of Cyber Security Circle

RISK DIALOG / RISK ASSESSMENT

COMMUNICATION DATA OWNERS / AUTHORITIES

CRISIS PREVENTION

LEGAL COUNSELING

IT FORENSICS

Offer within the scope of a Cyber Protect Policy:
• Review, optimize or newly create a cyber crisis management plan
• Cyber crisis management within 48 hours
• Cyber crisis exercise
... AND IN A LOSS EVENT?

Whether the company’s own losses or damage incurred by third parties – at AGCS, cyber incidents are processed by a “single source”.

As soon as you ascertain a cyber incident, contact us as quickly as possible – via the Allianz Cyber Emergency Hotline (24/7).

We can help you decide what to do next and consider – together with you – which service providers from our Cyber Expert Network are best able to assist you with these steps.

Our service providers will contact you within a few hours to plan the next steps together with you. The costs for the various consultancy services are covered within the scope of the Cyber Protect Policy (service agreements with AGCS).