MANAGING CYBER-RISK
Cyberthreat intelligence & the Insurance sector
OCTOBER 2018
Cyberattacks on the insurance industry are increasing, with criminals moving away from the banking sector towards targets with different levels of cybersecurity maturity.

Poor cyber-risk management can lead to fines, closed accounts and brand devaluation.

Cyberthreat visibility both inside and out of the network must be considered to protect the business.

Managing cyber-risk is like managing your clients' risk. It is not a binary of whether you get attacked, but a spectrum of how likely it is an attack will happen.

Introduction 6

What is cyber-risk management? 7

What sort of data is at risk? 7

State of the Industry 9

Trends 10

Malware 10
DDoS attacks 11
Cryptominers 12
Ransomware 12
Hacktivism 13
Insurer-driven risk 13
Site impersonation & spoofing 14

Regulation and Legislation 14

Cyber-risk management 15

The role of the insurance broker 15
5 questions for the business executive 16
5 questions for the security executive 16

The role of threat intelligence 17
Large-scale insurers 17
Mid-size insurers 17
Small-size insurers 17

The benefits of real-time, dynamic threat intelligence 18

Credentials 19
Domain protection 19
Social media 19
Data leakage 19
Hacktivism 20
Mobile apps 20
Dark web 20
Scoring 20

Conclusions 21

Endnotes 22
Cyberattacks on the insurance industry are increasing, with criminals moving away from the banking sector towards targets with different levels of cybersecurity maturity.

Managing cyber-risk is like managing your clients’ risk. It is not a binary of whether you get attacked, but a spectrum of how likely it is an attack will happen.

- **3 per month**
  - Average number of effective attacks on Insurers (Accenture)

---

**Data at risk**

- Corporate assets
- Login credentials
- Personally Identifiable Information (PII)
- Financial assessments
- Business plans
- Customer financial details

---

**$148**

- Average cost per lost or stolen record (Ponemon)

---

Poor cyber-risk management can lead to fines, closed accounts and brand devaluation.
The nature of the data necessarily gathered by insurers is highly valuable to cybercriminals - increasingly liabilities in the event of a successful attack.

Under GDPR insurers have a high level of risk, and should invest in cybersecurity tools and solutions to minimize the impact of attacks on the enterprise.

37% of insurers have a clear cybersecurity chain of command (Accenture).

There are various options available to detect and respond to new, emerging and existing threats for insurers:

- Large insurers use Security Operations Centers (SOCs), external vendors, supported by threat intelligence for realistic attack simulations.
- Mid-size insurers operate with a number of teams with limited resource, outsourcing threat gathering process.
- Smaller insurers enlist services of MSSPs to handle many cybersecurity needs.
Insurers use threat intelligence to accelerate threat detection, prioritization and incident response capabilities, and focus scarce resource where it is needed.

### FOR THE BUSINESS EXECUTIVE

- Allocate enough budget to cybersecurity in your business strategy
- Establish a chain of command and escalation path in event of a breach
- Know what assets are of value to cybercriminals and protect them
- Demonstrate full compliance with relevant regulation and legislation
- Demand same cybersecurity standards of all third-party suppliers

### FOR THE SECURITY EXECUTIVE

- Demonstrate importance of a robust security posture
- Rationalize your cybersecurity budget and spend where you need to
- Maintain high level of cybersecurity education at all levels in organization
- Regularly audit security protocols with sufficient patching, pen-testing, red-teaming
- Leverage actionable threat intelligence and analytics

---

- Credentials
- Social Media
- Data Leakage
- Dark Web
- Hacktivism
- Mobile Apps
- Scoring
INTRODUCTION

Organizations in all sectors face increasingly virulent and sophisticated cyberthreats on a weekly, if not daily basis. The insurance sector is particularly at risk. From organized criminal groups seeking PII (personally identifiable information), financial account data and anything else that can be monetized, to hacktivists trying disrupt the day-to-day business of their target, to APTs (advanced persistent threats) gathering intelligence and information to attack operations and customers, insurers large and small are often a long way behind the curve when it comes to shoring up their security infrastructure.

In part, this is due to attackers moving away from the financial sector as they seek weaker targets. Yet these targets still have a huge amount of data points on the individuals and enterprises they deal with. Combined with distributed service models and increased digitization of services, the risk across the insurance value chain continues to grow.

This whitepaper will focus on the issues that confront the C-suite in the insurance industry, offering insight and guidance to meet the challenges they face today.

It’s a bold claim, but in today’s cybersecurity landscape, prevention doesn’t work. You only need to look to recent headlines to see that the number of high-profile breaches has been increasing over the past few years, even for organizations who invest millions in cybersecurity. Managing cyber-risk is like managing client risk – it is not based on a binary of whether you get attacked, but exists a spectrum of how likely it is that an attack will happen.

The frequency and severity of cyberattacks across all sectors increases and insurance is no exception. Given the sensitivity of the information held by insurers, the risk of attack is even higher. Take Anthem and Premera Blue Cross, for example, who had millions of customer records compromised in recent years, damaging their reputation as well as putting their clients at risk.

A proactive, resilient cybersecurity posture is necessary to protect the enterprise, its customers and their data. The following pages set out the cybersecurity landscape for insurers, offering insight around trends, regulations, responsibilities for companies of all sizes, and finally the proactive steps that insurers can take to manage their cyber-risk effectively.

Cyberattacks on the insurance industry are increasing, with criminals moving away from the financial sector towards weaker targets.

Managing cyber-risk is like managing your clients’ risk. It is not a binary of whether you get attacked, but a spectrum of how likely it is an attack will happen.

A proactive, resilient cybersecurity posture protects the enterprise, its customers and their data.

Use this whitepaper to assess the threat landscape, learn about trends, your responsibilities as an insurer, and steps you can take to manage cyber-risk.
Cyber-risk management must be comprehensive and cover cyberthreats which are deliberate and planned, as well as those unintentional blunders which can cause damage to the enterprise.

Risk management has become somewhat of a catch-all phrase in cybersecurity, due to the range of services and approaches on offer. This section will clarify what cyber-risk is (and isn’t) and why the technologies that support it are critical for organizations in the insurance and financial services sectors.

The Institute of Risk Management defines cyber-risk as “any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its IT systems.” Meanwhile, according to RSA, it is “the potential loss or harm related to technical infrastructure or the use of technology within an organization.” Clearly, both these definitions are quite broad.

Exposure to risk should not only be based on intentional breaches and attacks on IT systems. Deliberately malicious attacks carried out by cybercriminals have the goal of stealing confidential customer data through cybersquatting a domain, compromising credentials through a malware infection, or conducting BEC (Business Email Compromise) through a spearphishing attack. These sorts of premeditated attacks are concerns that all companies must manage. However, unintentional data leaks, internal user errors, mistakes made when configuring systems, and careless third-party partners also contribute to cyber-risk.

As a result, cyber-risk management must be comprehensive and cover cyberthreats which are deliberate and planned, as well as those unintentional blunders which can cause damage to the enterprise. The ubiquity of this risk means that all areas of an insurer’s business and organization are under the spotlight, and so a risk management program – no matter how large or small the enterprise – is extremely important.

WHAT SORT OF DATA IS AT RISK?

The threats to insurers and financial services have much in common with any business, but there are specifics relating to their industry that put them at higher risk.

On the business side, there are confidential business plans, financial assessments, and other important company-related data which must not get into the wrong hands. Compromised employee login credentials can lead to account takeovers, identity theft, blackmail, spreading crimeware, fraud and other criminal activities (see our in-depth report into the Credential Theft Ecosystem for more detail). Sophisticated phishing campaigns targeting VIPs and employees have been known to cause havoc for an organization, while targeted malware against IT infrastructures of these organizations have also been discovered in the wild.

Imagine a scenario where employees were hit by a phishing campaign that contained stealer malware and successfully compromised login credentials, and subsequently through lateral movement, its internal servers. Verizon’s DBIR 2018 records that 4% of people will click on any given phishing campaign. So even if the attack only affected a few employees, it only takes one compromised credential to enter the infrastructure and persist, causing
Customer data at risk:

- Banking details
- Login credentials
- PII

Inadequate cyber-risk management can lead to fines, closed accounts and brand devaluation

Cyberthreat visibility both inside and out of the network must be considered to protect the business

On consumer-facing side, insurers and financial services companies are at even greater risk than most due to the nature of the information they hold – this is a fact that cybercriminals are acutely aware of. Compromised customer records and other PII make clients particularly vulnerable to exploitation. These include bank details and medical records, and their theft can and does have a knock-on effect on the enterprise, as well as causing a huge amount of pain to those directly affected. Incidents which result in the exfiltration of this sort of data can have a huge business impact.

Take a successful cyberattack which exfiltrated a company database of customers and sales prospects’ social security numbers. Cybercriminals then seek to sell the data on the black market, while the insurer would be obliged to reimburse all damages to those affected as well as suffering significant brand devaluation publicly.

Another example would be software vulnerabilities that had not been patched in time, or a customer database which didn’t use a sufficient level of encryption. An attacker exploits either of these vulnerabilities and exfiltrates payment information for customers, impacting the company’s bottom line in compensation costs, not to mention significant reputational damage. Even further, the company then gets hit by GDPR penalties for not taking responsible steps to comply with the requirements of the legislation.

In summary, inadequate cyber-risk management can lead to fines, closed accounts and brand devaluation. Cyberthreat visibility both inside and out of the network must be considered to protect the business.

Immediate costs

These are the largely unavoidable costs that include the immediate business and media impact, plus the cost of restoring the confidentiality, integrity and availability of data and systems.

Immediate costs include:
- Forensic investigation costs
- Legal costs
- Customer notification costs
- Credit monitoring for customers
- Potential business interruption costs
- Public relations expenses
- Fraud costs
- Extortion costs
- Physical damage costs
- IT/business remediation costs

Slow-burn costs

These vary according to the type and severity of the event, and how it is handled, but typically include the long-term business impact and costs incurred by reimbursing victims, as well as reparation and the payment of penalties for failure to meet obligations.

Slow burns costs include:
- Third-party litigation expenses
- Customer churn from reputational damage
- Regulatory fines and penalties
- Share price impact
- Loss of management focus
- Loss of competitive advantage
- Loss of revenue

Time from event discovery

Fig. 1 This graphic from KPMG illustrates the impact of a successful cyberattack on a business.12
STATE OF THE INDUSTRY

According to Accenture, a typical insurance organization faces more than three effective attacks per month, yet four fifths of the larger insurers’ security executives were confident in their cybersecurity strategies. Yet in another report from EY, almost half of insurers have discovered “significant” cybersecurity incidents within their organization. Clearly, there is a disconnect between confidence and capability.

As outlined above, companies in the insurance industry remain high-profile targets for cybercriminal organizations, hacktivists and APTs. The sector continues to migrate towards digital channels to create closer customer relationships, driving highly-integrated platforms and portals, online application and claim enablement forms, as well as a whole gamut of app-based systems. As a result, the number of attack vectors available to cybercriminals has expanded and threaten companies which traditionally do not have a huge amount of experience working in such a high-risk environment. The average cost per lost or stolen record is recorded at $148, with data breaches continuing to be costlier year over year.

Unfortunately, the odds are stacked in the favor of the attackers. They do not have to invest a great deal to breach an organization, whereas insurers must allocate considerable resource to defend their assets.

There have been a number of high profile breaches in recent years. In early 2015, Anthem, the second-largest health insurer in the US, had up to 80 million customer and employee records exfiltrated. According to EY, the financial impact is expected to surpass its own cybersecurity policy, covering losses of up to $100 million.

11 million customers’ PII was stolen from Premera Blue Cross and was announced in March 2015, which had a hugely negative reputational and legal impact on the insurer. Emphasizing the significance of the breach, it has only recently emerged that the insurer intentionally destroyed evidence in the case despite ongoing litigation against it, several years down the line.

One of Arizona’s largest healthcare providers, Banner Health, saw 3.7 million patients’, customers’ and doctors’ PII stolen in a breach that commenced on 17 June 2016. A class action lawsuit is still ongoing there too.

Below are some recent trends identified by Blueliv providing valuable information to insurers seeking to enhance their security posture.
Malware stealers are widely-used by cybercriminals to acquire sensitive information. The first graphic displays the top malware types that Blueliv has detected recently which have been targeting insurers.

Trojans have multiple functionalities that allow them to steal the victim’s information, such as man-in-the-browser techniques, keystroke logging, and form grabbing. Blueliv monitors botnet configurations as new functionalities have started to spread among banking trojans in recent years. These functionalities include webfilters, dnsfilters and webinjects. These functionalities are defined and detailed in our recent report on The Credential Theft Ecosystem.

The following chart shows the number of unique trojan samples detected by Blueliv that are actively targeting insurers and other financial entities. It also displays the amount of related C&C servers which, in combination with the samples, provide an estimation of the complexity of the botnet and the level of threat that it entails.
Attackers attempt to get hold of users’ credentials through tampered login panels and perform fraudulent activities in their name.

Cybercriminals have been known to use backdoors to install custom malware and move laterally within a network in order to mine sensitive data.

DDoS attacks are a significant risk to insurers through disruption, combined with remediation costs and customer compensation.

These samples are mostly distributed through spam mail campaigns and exploit kits, which usually employ a loader to drop the actual trojan. This distribution process is rigorously detailed in our report Chasing Cybercrime: Network insights into Vawtrak v2. It is available online and provides deeper insights about these infection methods.

A webinject is a technique used to intercept data after it is decrypted from SSL but prior to its display in the browser. Consequently, it gives the trojan the ability to modify the response of a webpage’s server. That response is leveraged by trojans to request further information from the victim to perform fraudulent transactions, among other activities.

The main targets of this type of attack are organizations in the insurance and financial services sectors. The perpetrators perform these attacks in an attempt to get hold of users’ credentials through tampered login panels and perform fraudulent activities in their name.

It should be noted that another potential danger for insurers are bots which have already infected the system through a different vector. For example, cybercriminals have been known to use backdoors to install custom malware and move laterally within a network in order to mine sensitive data. Threat intelligence is crucial, not just for looking outside the network, but seeing what’s already inside too.

**DDoS Attacks**

In the first months of 2018, we witnessed the largest ever distributed denial of service (DDoS) attack hitting a record 1.7 Tbps; it was not that long ago when the previous record of 1.3 Tbps was set. It is predicted that many insurers will be targeted with DDoS attacks to paralyze their systems and open the door to cybercriminals.
This time, a new type of DDoS used secured memcached database servers to amplify attacks against a target. Installed by default on many Linux operating system versions, memcached is designed to cache data and ease the strain on heavier data stores, like disk or databases. It is typically found in cloud server environments and it is meant to be used on systems that are not directly exposed to the Internet.

These types of attacks are a significant risk to insurers, since revenue will likely be disrupted as a direct result of an attack. Furthermore, costs for remediation and customer compensation should be added to the bill. We expect that DDoS attacks will continue in the coming months, perhaps even reaching 2 Tbps, and they will start to include more ransom demands to increase their financial benefit.

**CRYPTOMINERS**

Cryptocurrencies, due to their surprising fluctuations at the end of 2017, have increased in popularity globally and sparked interest in new mining methods. Blueliv has observed several threat actors using websites to exploit the visitors’ CPU power to mine for them, and attackers are no longer limiting themselves to personal computers, setting their sights on other more powerful computational resources including web servers.

The attackers focused on cryptomining may not earn a large amount of money in a short period, but over time they can acquire huge amounts. Meanwhile, their mining pool negatively affects the hosts’ performance due the computational overload.

The level of processing power used by many insurers is very attractive to cryptominers, and the sophistication of mining software means that an infection may go undetected for many months. With a Monero miner using XMRig, for instance, cybercriminals programmed it not to run the mining process hourly, but to download the whole malware payload every hour. This allows the attackers to halt the mining infrastructure if they feel that they are about to be caught, cutting the next round of payload downloads and deleting all traces from their victim’s systems.

We expect to see more blitz campaigns in the coming months, exploiting unpatched known vulnerabilities, which could be easily avoided by patching old servers and deploying relevant security measures.

**RANSOMWARE**

Ransomware continues to be a significant risk to organizations across the globe, as multiple alerts of new and improved campaigns suggest. Ransomware developers always focus on extracting as much profit as possible from their victims. Examples include Thanatos’ developers, who made the first ransomware to accept Bitcoin Cash as a payment method, or the rising use of Ransomware-as-a-Service.

Ransomware-as-a-Service is a business model where ransomware software can be leased to any client willing to pay the price. Instead of developers using the malware exclusively, they offer its usage to third parties for an affordable price or by receiving a percentage of the proceeds.

This business strategy makes RaaS a particularly dangerous threat due to its indeterminate client base. From regular users with bad intentions to companies interested in disturbing the performance of their competitors,
anyone with the ability to pay could be a potential threat actor.

Often RaaS developers try to make their products attractive for unskilled users, creating intuitive online management portals for deploying and tracking the rented ransomware. They even let clients configure some parameters, such as the ransom price or message shown to the victims.

Just like regular software business models, some RaaS even have their own customer support teams, helping clients use the software by solving issues. Even though RaaS is a new trend per se, during the past quarter three new types have appeared as services: GrandCrab, Saturn and Data Keeper.

This model of cybercrime business is win-win for malware developers; they develop powerful yet easy-to-use software for others to deploy, and they receive a cut of the proceeds. It should be noted that it may not always be a highly profitable business, as it could depend on the number of victims willing to actually pay for recovering their files, but the potential risk to the creators getting caught is far less in comparison to more popular malware. RaaS may not represent the largest part of the ransomware scene, but it is steadily growing and we can expect it to gain more attention over time.

Insurers should be particularly cautious about ransomware, given the highly competitive landscape of their marketplace and importance of reputation. Customer bases can be unstable and cancel policies en masse if they do not trust the organization. In a different vein, the nature of the data possessed by insurers means that they are highly targeted by cybercriminals using ransomware, and therefore should lay on appropriate defense measures.

**HACKTIVISM**

The insurance sector is increasingly high profile. Though companies of all sizes are competing against each other in the marketplace, hacktivists may not make the same differentiation and attack any insurer as a result of grievances held against a particular organization. If a major company is involved in some controversy, the knock-on effect could be significant across the sector. Where hacktivists fail to penetrate one company, they might have better luck at their competitor, drawing attention to the weaknesses of the sector as a whole — and causing significant reputational damage in the process.

**INSURER-DRIVEN RISK**

Many insurance companies are investing heavily into consumer services and mobile applications to support their customers. The more services there are, however, the broader the attack surface and window of opportunity for attackers. These are becoming more heavily targeted, relying as they do on the use of customer credentials and comparatively lower defenses than major banks.

Outsourcing agreements specifically hand over control of important assets and data to third-party providers. While this may provide business benefits, it also increases the risk of these assets being compromised, since the security protocols of the third-party suppliers may not be as robust as the insurer.

Moreover, the nature of the data necessarily gathered by insurers is highly valuable and this cannot be understated. It is one thing to store a username, password and credit card details. However, medical histories, financial situations and other extremely personal data is also collected, and the more that is gathered, the greater liability in front of data protection legislation.
SITE IMPERSONATION & SPOOFING

Fake websites pose a real risk to insurers. The surge in businesses taking their services online presents new opportunities for cybercriminals to exploit. The broader the service offering, the higher the risk, since the insurer will necessarily have a greater number of URLs which can be impersonated. If, for example, an insurer offers services (like logistics, for example) which nominally use the brand, then their exposure is greater as customers may trust the site without questioning the authenticity of the page.

For example, a carefully crafted spoof site for an insurer will adopt the design of the target site, logos, fonts, tone of voice and often will have a similar URL – or one that looks legitimate enough to convince the visitor that the site is safe. The replica site may be used for a variety of purposes, including advanced phishing campaigns, spreading malware and capturing visitor information which can later be used for malicious purposes. The level of potential fraud, through illegitimate credit card usage or bank transfer, is also high. It is important to increase resilience both internally and externally, by investigating potential site impersonations through threat intelligence and taking them down as soon as possible to protect the brand.

REGULATION AND LEGISLATION

Generally speaking, financial services and insurance organizations worldwide are subject to a considerable amount of cybersecurity compliance regulation. This legislation not only regards data privacy for consumers, but also places obligation on companies themselves. The EU GDPR, for example, enforces that companies should “implement appropriate technical and organizational measures to ensure a level of security appropriate to risk.”

Given that insurers have a high level of risk, there is a significant onus on them to invest in cybersecurity tools and solutions to minimize the impact of cyberattacks on the enterprise that could affect their business and customers.

Though the impact of GDPR is worldwide – dealing with all organizations which have customers or do business within the EU – US institutions also retain their own guidance principles. The National Association of Insurance Commissioners, which sets standards for the industry in the US, released non-binding principles in 2015 which expected companies to ramp up their security controls. One of these principles encourages insurers “to stay informed regarding emerging threats or vulnerabilities, as well as physical threat intelligence analysis and sharing.”

It is clear that in recent years a greater understanding of cyber-risk has forced relevant regulatory bodies to take affirmative action. Though compliance requires significant investment, responding to these challenges encourages a greater understanding of cyber risk and a more effective approach. For more detail on how threat intelligence can mitigate the impact of GDPR, see our special whitepaper here.
From a technical perspective, insurers are under constant pressure to modernize their infrastructure. However, this rush to innovate has its own pitfalls when it comes to managing cyber-risk, not least the increased emphasis on keeping critical data highly secure yet immediately available.

The Role of the Insurance Broker
It is surprising that just 37% of insurers have a clear cybersecurity chain of command, according to Accenture. Given that insurers’ business depends on risk management, it appears that structures for accountability, oversight and effective response in their own houses may require stronger foundations. Insurers should therefore seek to ask questions of themselves in order to better manage their cyber-risk. These can be divided into two categories – one relating to business, the other to the technical side.
Cybersecurity priorities for CEOs, CFOs and Legal should be different from CIOs and CISOs

5 QUESTIONS FOR THE BUSINESS EXECUTIVE

CEOs, CFOs and Legal should ask the following:

1. How integral is cybersecurity to our business strategy? Are we allocating enough budget?
2. Do we have an established chain of command in the event of an incident, and is there a detailed escalation path when an incident happens?
3. Do we have an understanding of why we are targeted by cybercriminals? What do we have in our systems which they’re trying to get at?
4. Can we demonstrate full compliance with the relevant regulation and legislation?
5. Do we demand the same standards we set for ourselves of all the third parties we work with, who have access to our systems?

5 QUESTIONS FOR THE SECURITY EXECUTIVE

CTOs, CIOs, CISOs and other members of the IT team should ask the following:

1. Do the rest of the management understand the importance of a robust security posture? Do they budget enough for it and recognize the ROI?
2. Have we rationalized the way we budget for our external products? Are we spending too much in the wrong areas relating to our business?
3. Are we doing enough to educate the entire organization about the importance of cybersecurity?
4. Are we auditing our security protocols often enough with sufficient patching, pen-testing and red-teaming, and are we sufficiently validating each and every new digital product we produce?
5. Are we leveraging actionable intelligence and analytics?

Overall, it is critical to create a strong culture of cybersecurity within the organization. This should extend from the management team all the way down to the newest hires, with encouragement to fully understand the risks of using certain technologies. Frequent company-wide training is encouraged, and though cybersecurity education is important in any enterprise regardless of size, a robust risk culture in larger companies is particularly important simply because of the scale of both technology and staff. Risk increases due to the greater probability of insider threats too, so a strong culture of risk reporting and increased interaction between departments, smoothing the flow of information, is also supported.
THE ROLE OF THREAT INTELLIGENCE

Threat intelligence is actionable information, delivered in an automated way so that organizations can detect threats both inside and outside their network, and prioritize their responses. The reason it is so important is that it allows security teams of all sizes to focus their resources – which are often limited – on the most crucial threats targeting their networks and infrastructure.

Most IT teams lack the technology and resource to automate threat collection, correlation and analysis, and instead rely on log data collected by their critical infrastructure. This data is not provided in real-time, and in a constantly evolving threat landscape, the level of cyber-risk remains extremely high.

Threat intelligence is also extremely effective in helping identify and protect critical assets. It can help insurers define what is of interest to attackers, where these assets are located, and how they can be accessed. Armed with this information, security teams are able to put in place appropriate defense measures ahead of time.

Depending on the size of the insurance company and level of investment into their security resources, there are a variety of options available to detect and respond to new, emerging and existing threats.

LARGE-SCALE INSURERS

The largest companies are likely to have broad functioning security teams, most probably including a security operations center, or SOC, of their own (in addition to external vendors). They are encouraged to conduct regular maturity assessments and red-teaming activities to identify potential weaknesses before the bad guys do. Conducted on a routine but irregular basis, red-team attacks are an immensely valuable method to strengthen an organization’s security conditioning. They are supported by threat intelligence companies who can provide the most up-to-date TTPs (tactics, techniques and procedures) for realistic attack simulation.

MID-SIZE INSURERS

These organizations probably have a SOC, but if not, they operate with a number of relatively small teams (cyberincident response teams/CIRTs, Threat Intelligence teams) with limited resource. Given the numerous challenges in gathering threat intelligence ‘in-house,’ many small- to mid-size insurers tend to use external threat intelligence services. It means outsourcing the gathering process and receiving actionable data.

SMALL-SIZE INSURERS

It is unlikely that these organizations have the budget for a SOC, and it is unlikely that they even use threat intelligence services. Indeed, external threat intelligence vendors often appear to be well over budget, with smaller firms simply unable to handle the recurring expense. However, this is inaccurate: effective and timely threat detection and prioritization is available to even the smallest of insurers. For these organizations, it is usually most cost-effective and sensible to enlist the services of a managed security service provider (MSSP), who can handle many if not all their cybersecurity needs.
Quality threat intelligence helps accelerate threat detection, prioritization and incident response capabilities. Trying to detect threats is like looking for the proverbial needle in the haystack. Sorting through false positives and the reams of data that you collect, combined with ever-more sophisticated TTPs employed by cybercriminals, means this haystack isn’t getting any smaller. Threat intelligence means that you can focus scarce cybersecurity resources on where they are most needed.

The risk of successfully using attack vectors outlined earlier in the document may all be mitigated using actionable, dynamic threat intelligence.

Fig. 3. How Blueliv gathers and process data from millions of sources in the open, deep and dark web, extracting what is relevant to you.
Real-time threat intelligence can also help you maintain visibility of the threat landscape so that your security infrastructure is able to respond to the latest threats, in real-time. This includes detecting malicious activity already inside your network, analyzing it and helping your security team understand the attackers’ objectives.

As outlined above, many insurers are yet to see the value of adding threat intelligence to their cybersecurity infrastructure, as a crucial layer of deep defense. In part, this is due to the misconception that the expense is significant and not worth the ROI.

This may be true of vendors who push a one-size-fits-all approach – you either buy or you don’t. On the other hand, the clear benefit of cyberthreat intelligence delivered through modules is that it works to a pay-as-you-need model. Insurers are able to select the modules which are most relevant to their business and plug the gaps in their cybersecurity infrastructure. Below, Blueliv modules relevant to insurers are briefly outlined.

**CREDENTIALS**

Credentials are the gateway to an organization’s infrastructure, and it only takes one compromised password to cause havoc. This module identifies leaked, stolen and sold user credentials in real-time on the open, deep and dark web, along with information about relevant malware used to steal it. A combination of sinkholes, honeypots, crawlers and sensors are continuously searching for compromised credentials – the sooner these are identified, the sooner they can be retrieved, and the impact mitigated.

Crucially, this includes the identification of stolen credentials of customers and partners of a company, i.e. individuals outside the network. Targeted Threat Intelligence is the only way to identify stolen login data outside your company’s perimeter. However, the threat is extremely high since hackers use stolen credentials in a majority of successful breaches.

**DOMAIN PROTECTION**

Fraudulent domains are a risk to insurance organization and end customers, with the goal of stealing information and damaging the brand. Effective phishing campaigns and cybersquatting can be mitigated by proactive detection, where insurers can take effective countermeasures. Additionally, insurers can protect and prepare corporate VIPs against phishing and social engineering attacks, since they tend to be the biggest targets.

**SOCIAL MEDIA**

Insurers should ensure that trust in their brand remains high. Social media and search engine monitoring of an organization’s digital footprint helps find websites not authorized to use the brand, logos, assets claiming partnership affiliation assets and more, so insurers can take proactive steps to shut them down.

**DATA LEAKAGE**

The larger the organization and the more third-parties it engages, the greater risk it has to manage. This module monitors whether an organization’s sensitive documents have been leaked on the internet, deep web or P2P networks, intentionally or otherwise.
MANAGING CYBER-RISK – THE BENEFITS OF REAL-TIME, DYNAMIC THREAT INTELLIGENCE

**HACKTIVISM**
By monitoring global hacktivism activity on social networks, the open and dark web, insurers can protect their infrastructure before a potential attack happens. Using an advanced early-warning system and active geolocator, the module generates targeted threat intelligence to shield against potential attack vectors.

**MOBILE APPS**
As more insurers create new digital platforms to engage with clients, cybercriminals are busy creating malicious and illegal applications, hiding in plain sight in non-official marketplaces. They lure away customers and steal valuable data, with the potential to have a significant negative impact. This module specializes in detecting applications claiming affiliation to insurance organizations or using company assets without authorization, to protect both brand and reputation.

**DARK WEB**
Insurers would do better to boost their awareness of what’s going on in the underground, observe malicious activities targeting their organization and proactively prevent future attacks. This module delivers a serious advantage to security teams by putting a spy in the enemy’s camp: insurers become better informed about criminals targeting their organization and customers, can proactively prepare countermeasures, and find already-compromised data before the impact is too severe.

**SCORING**
Perhaps most relevant to insurers, targeted risk scoring modules can work both to protect the insurer, and also check on potential enterprise clients. Using this module, insurers can evaluate the customer, see how big a potential risk they carry, and calculate conditions based on this information.

Furthermore, threat intelligence that provides scoring capabilities can be used effectively to define your attack surface. This is the total sum of the vulnerabilities that are accessible to a cybercriminal and is not limited simply to entry points. Scoring enables organizations to monitor and protect those attack surface areas which are exposed, from individual employees, domains, IPs to external parties in the supply chain.
Ultimately it all comes down to making the right investments. Insurers need to try and stay one step ahead of their attackers. Innovation within the company and collaboration with external suppliers helps assess and strengthen cyber resilience in critical areas.

Blueliv has been working with very well-known insurers for many years, building a deep understanding of their strategic cybersecurity needs and the industry-specific threats they face.

And while cybersecurity strategies within the insurance sector are maturing, there are still many improvements that can be made. Investment efficiency, combined with an understanding of the importance of security from the top down, should drive the right allocation of funding depending on requirements. Modular, pay-as-you-need cyberthreat intelligence provides a robust platform with which to complement insurers’ existing cybersecurity setups, whatever the size of the organization.

In sum, proactive threat detection and monitoring through threat intelligence should be supplemented by a process of continuous cyber-hygiene within the organization. This can help prevent attacks, as well as mitigate their impact when one happens. Setting the appropriate alerts which detect intrusions can offer some protection, but an ongoing process of pentesting and patching is crucial for safeguarding the insurance company. The bad guys are constantly testing new ways to exploit your infrastructure, so remaining static when it comes to your security protocols is a sure-fire way to get breached. This includes performing periodic internal security reviews, red-teaming, and an ongoing process of education among all employees.

Cybersecurity is everybody’s job – not just the remit of the IT team. By establishing and promoting an appetite for cyber-risk management, insurers will find themselves better protected against the bad guys. In fact, the best way to fight cybercrime is to operate in much the same way as the bad guys. Where they build communities to exchange information and TTPs, so must we.

Blueliv hosts a global community of thousands of cybersecurity experts and encourages them to share news, views, IOCs and more – the Blueliv Threat Exchange Network. It gives members access to our free proprietary elastic sandbox, a close-to real-time cyberthreat map and it encourages information sharing. The growing global community is free to join – the fight against cybercrime is a collaborative effort.
**ENDNOTES**

5. EY, 2017, Cyber Strategy for Insurers, p6
6. Ponemon Institute LLC, 2018, Cost of a Data Breach, p3
7. EY, 2017, Cyber Strategy for Insurers, p7
About Blueliv

Blueliv is a leading cyberthreat intelligence provider, headquartered from Barcelona, Spain. We scour the open, deep and dark web to deliver fresh, automated and actionable threat intelligence to organizations, helping protect their networks from the outside in. Blueliv’s scalable cloud-based technology turns global threat data into sophisticated, relevant intelligence. We enable organizations to save time and resource by accelerating incident response performance, providing user-friendly evidence accessible to all levels within cybersecurity operations teams. Our pay-as-you-need solution delivers an accelerated, predictive view of the threat landscape in real-time. We do not believe in a one-size-fits-all approach, and work together to configure a modular solution bespoke to your needs using separate intelligence modules, all backed up by our world-class in-house analyst team. Blueliv has been named ‘Threat Intelligence Company of the Year’ by Cybersecurity Breakthrough Awards, a Gartner ‘Cool Vendor,’ and Go-Ignite winner; in addition to holding affiliate membership of FS-ISAC for several years.