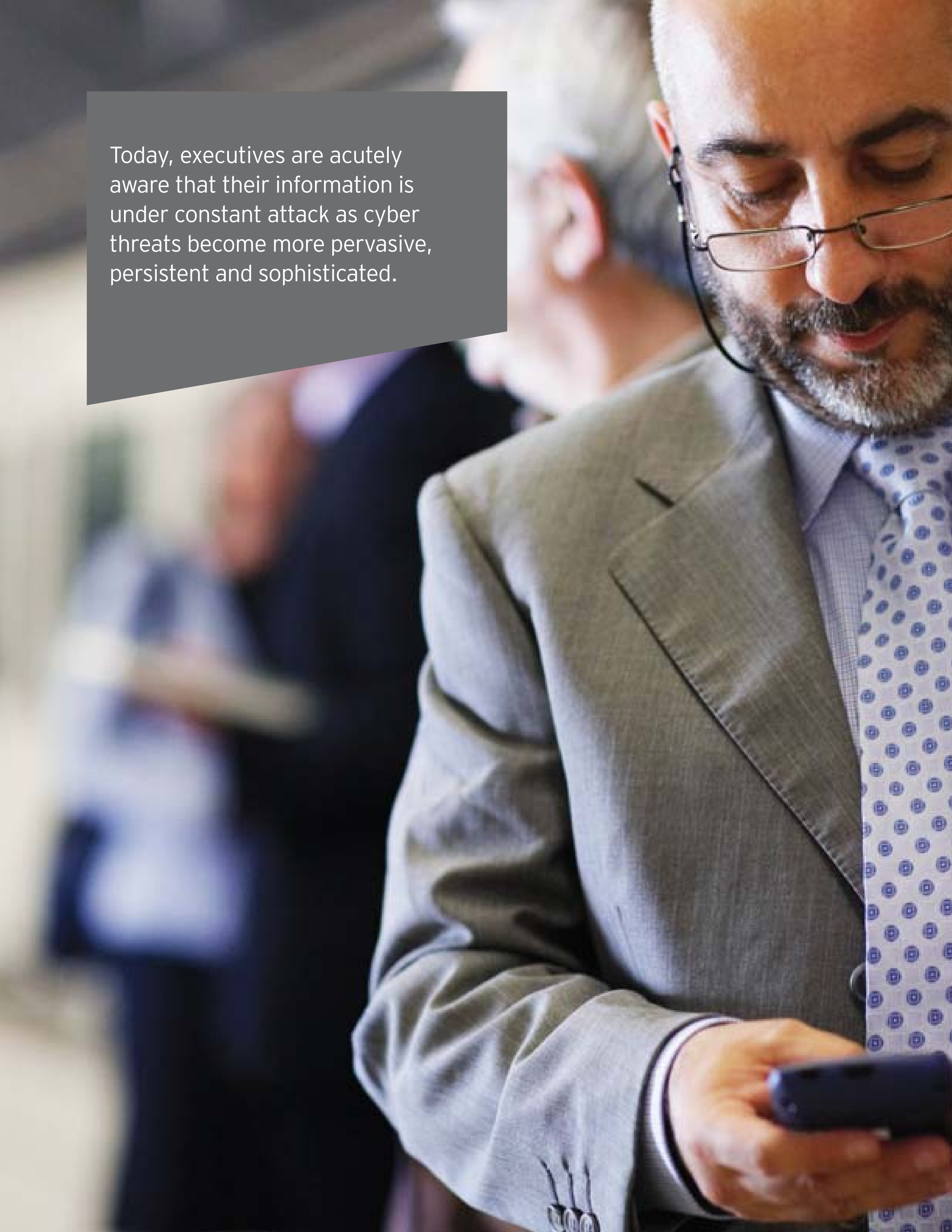
Cyber insurance, security and data integrity

Part 1: Insights into cyber security and risk — 2014

Building a better working world

Contents

Today, executives are acutely aware that their information is under constant attack as cyber threats become more pervasive, persistent and sophisticated.



Executive summary

This is the first in a two-part series on cybersecurity that focuses on both the data and risk aspects of this topic. It provides a broad view of why information security and cyber risk are so important for insurance companies and how they can protect their businesses from rapidly emerging threats.

In this paper, we look at the security aspects of cyber liability insurance, key issues that insurers face and the underlying security model that organizations should follow. Data integrity presents one of the biggest challenges for the industry and is a major focus of our discussion. Our soon-to-be-published second paper will explore the risk aspects of cyber liability insurance and look at how insurers and reinsurers are using mitigation in their risk assessments.

Corporations are increasingly exposed to cyber thieves and are the victims of corporate espionage (also known as the Insider Threat) caused by both internal and external security breaches. Fraudsters can be extremely capable of exploiting enterprise weaknesses and corporate defenses to steal intellectual property (IP), compromise corporate strategy, target customers, and pilfer or manipulate confidential and regulated information.

In the wake of numerous recent data breaches, much has been published on cyber liability insurance. Professional liability policies for companies providing computer hardware and software services have grown to include not just technology providers but all those collecting, storing and processing electronic data from their customers.

Key Contacts:

Shaun Crawford
Global Insurance Leader
Scrawford2@uk.ey.com

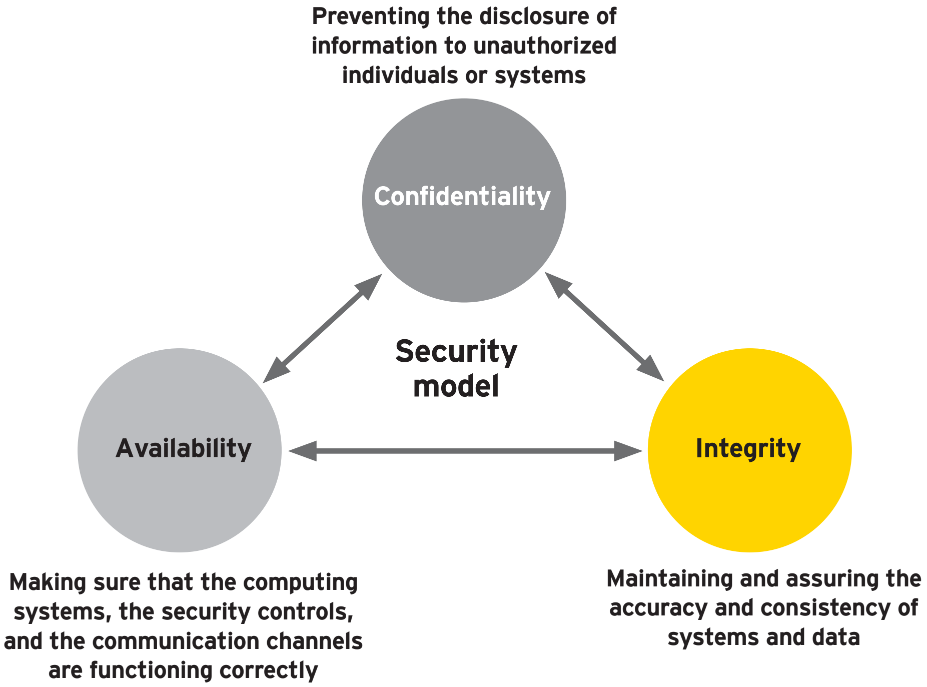
David Piesse
International Insurance Society (IIS)
Ambassador for Asia Pacific and
Insurance Lead at Guardtime
david.piesse@guardtime.com

Executives need to commit to improving information security if they are to achieve the intended benefits and demonstrate the value of their investment.

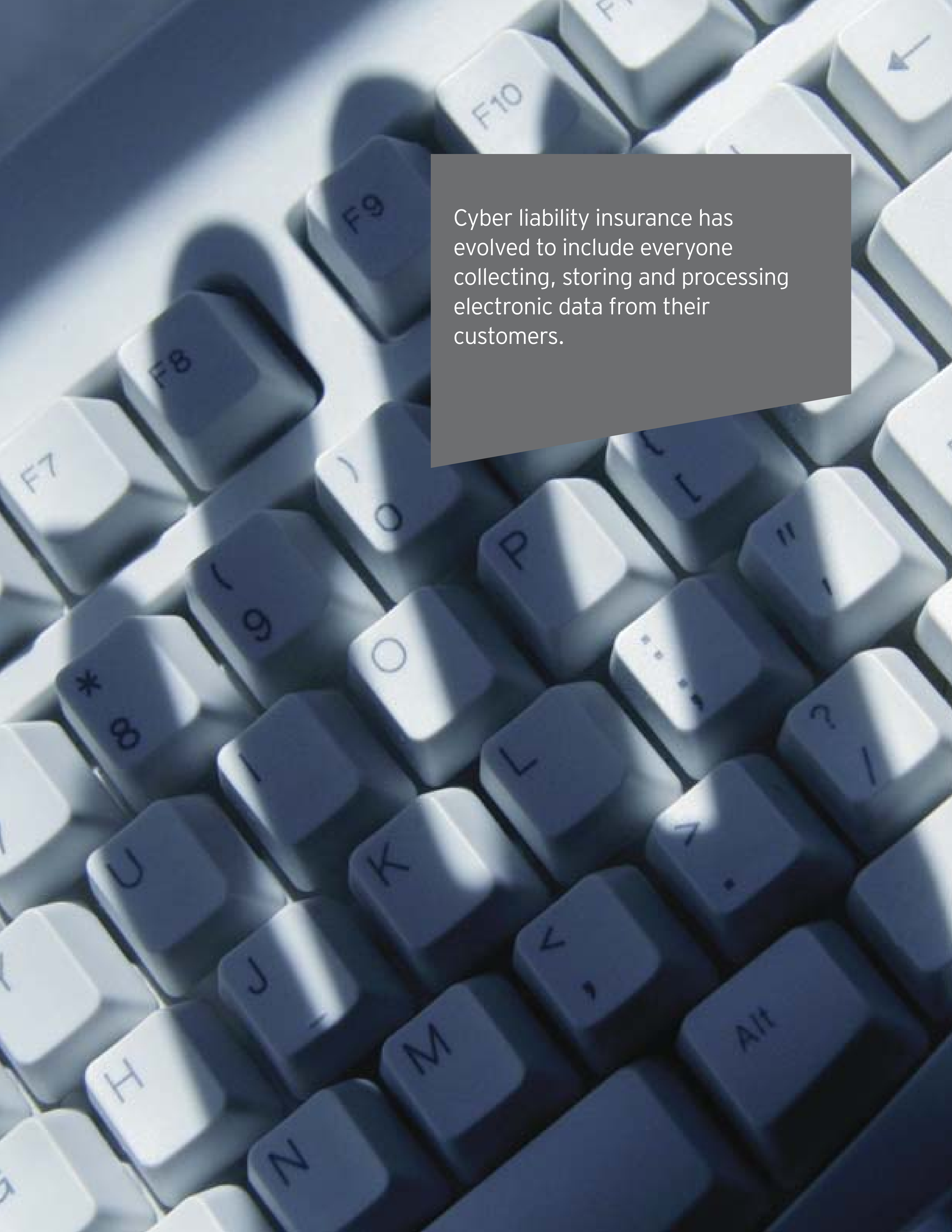
Pillars of information security

Security breaches can be categorized by a triad of confidentiality, availability and integrity, as shown in **Figure 1.**

Figure 1: Security triad


Preventing the disclosure of information to unauthorized individuals or systems
Confidentiality
Security model
Availability
Integrity
Making sure that the computing systems, the security controls, and the communication channels are functioning correctly
Maintaining and assuring the accuracy and consistency of systems and data

- **Confidentiality** prevents the disclosure of information to unauthorized individuals or systems. Close to 95% of all enterprise networks have been compromised by external attackers. Researchers revealed that only 3% of organizations felt safe against insider threats. Hundreds of millions of consumers have had their identity information compromised. The financial and reputational losses to businesses and shareholders stretch into tens of billions of dollars annually.
- **Availability** is making sure that computing systems, security controls and communication channels are functioning correctly. There are multiple security solutions on the market that address confidentiality and availability (denial of service). Large organizations have been amassing these solutions to address their operational risk.
- **Integrity** is maintaining and ensuring the accuracy and consistency of systems and data over the entire life cycle, and it remains the most nebulous, yet critical, pillar of the data security triad. Integrity is the gaping hole in security today. There is a media focus on confidentiality as it is easy to understand (a loss of customer information), but almost all losses of customer information have been caused by a breach in integrity (the introduction of malware compromising the integrity of the system used to secure the data). Integrity is a pre-requisite for ensuring confidentiality. Without it, encryption is worse than useless, bringing a false sense of security that almost always leads to downfall. Integrity brings auditability and transparency of evidence to governance frameworks that allow the public and private sector to mutually audit each other's activities in accordance with an agreed-upon governance framework.



Cyber liability insurance has evolved to include everyone collecting, storing and processing electronic data from their customers.

Introduction to emerging cyber threats

Financial institutions have developed innovative mobile applications that enable mobile payment transactions for their customers. While these applications represent innovation, the institutions never planned on supporting mobile banking. Consequently, digital exchanges via the mobile transaction network are at a higher risk of compromise and/or manipulation by exploiters with increasingly sophisticated tools and skills.

Moreover, infrastructure and storage outsourcing efforts supporting these applications put organizations further at risk as unregulated cloud service providers have highly differentiated security mechanisms that may not address threats to their customers.

Other challenges for insurers

- There is a stunning gap between the nature of new threats and the capabilities available to detect attacks, monitor (and stop) unauthorized exfiltration, and secure information.
- Few insurers have direct insights into the cyber liabilities surrounding intangible digital assets.
- Many do not have the tools to provide the direct real-time awareness necessary to calculate risks to insured digital assets stored by cloud service providers or enterprise networks.
- There is increased awareness that companies should be accountable for private records and the security of data collected from their customers.
- Insurers should make the fundamental assumption that any insured infrastructure will at some point be compromised, if not already. The more important and valuable the intangible (data) assets are (IP, customer and supplier base, etc), the more likely a compromise.

Policies and security measures

As exposure has evolved, so have policies. Since exposure exists for any organization that handles private information, insurance companies were tasked with creating a new type of policy. Most current cyber liability policies (or security and privacy policies) cover personal records in any format, including paper records. Other policies continue to emerge, such as contingent business interruption for cloud infrastructure that addresses more complex risks than data-breach-related exposure to data loss, theft or fraudulent disclosure.

From our experience, EY is seeing new distribution channels taking hold in rapid-growth markets in response to the exponential increase of mobile and digital devices. This is fostering new product development, along with security and privacy measures that are needed to protect companies in their adoption of digital technologies. Entering new markets generally requires new processes, systems, languages and cultures. These come with varying degrees of security risk and threat awareness.

The new issue on the table is electronic data integrity – how to independently prove what happened in a digital infrastructure, determine the impact of a security incident and distribute the liability for a data breach. This proof is hard to obtain when considering the internal information systems, and it becomes increasingly complicated with organizational reliance on outsourced cloud infrastructure and "trusted" administrators. New methods are needed to definitely identify the cause of compromise, the assets affected, when the compromise occurred, and if insured assets were exposed outside the organization.

Businesses must take a proactive approach to tackling cybersecurity rather than waiting for a breach to occur and then acting on it.

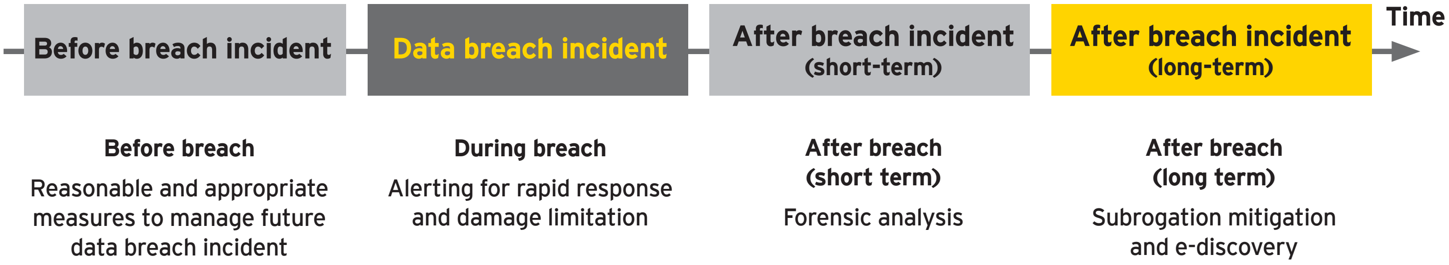
Data breach in cyber liability

In the real world, it would be considered reasonable and appropriate to require an independent audit of digital assets to be insured. In cyberspace, this is more challenging. Insurers have to rely on the insured to tell the truth about what assets have been impacted by a breach. Integrity standards for data enable insurance companies to conduct an independent audit of what digital assets exist (e.g., client data, IP) prior to a breach, thus preventing fraudulent claims.

Anatomy of a data breach

Data integrity standards can play a role in policy wording and risk assessments, as shown in the anatomy of a data breach **(Figure 2).**

Figure 2: Anatomy of a data breach



Before breach incident — **Data breach incident** — **After breach incident (short-term)** — **After breach incident (long-term)** → **Time**

Before breach
Reasonable and appropriate measures to manage future data breach incident

During breach
Alerting for rapid response and damage limitation

After breach (short term)
Forensic analysis

After breach (long term)
Subrogation mitigation and e-discovery

For stand-alone policies, these standards can be used as a warranty similar to a burglar alarm in a property policy. For cyber endorsements in original and other liability covers, such as errors and omissions (E&O), they could act as a simplified standard to insure small and medium enterprises (SMEs) for cyber liability when they cannot afford stand-alone cover. The extra cover, such as protecting digital assets against confidentiality and data integrity breaches, will allow carriers to increase their premiums because of a greater coverage and claims guarantee. It will also make the products more attractive to risk buyers.

Moreover, people have digital fingerprints via their mobile devices that identify them uniquely, and social media websites have turned this into an advantage in the sales process. Applying a unique data security signature associated with that fingerprint is bolstered with the data integrity standard.

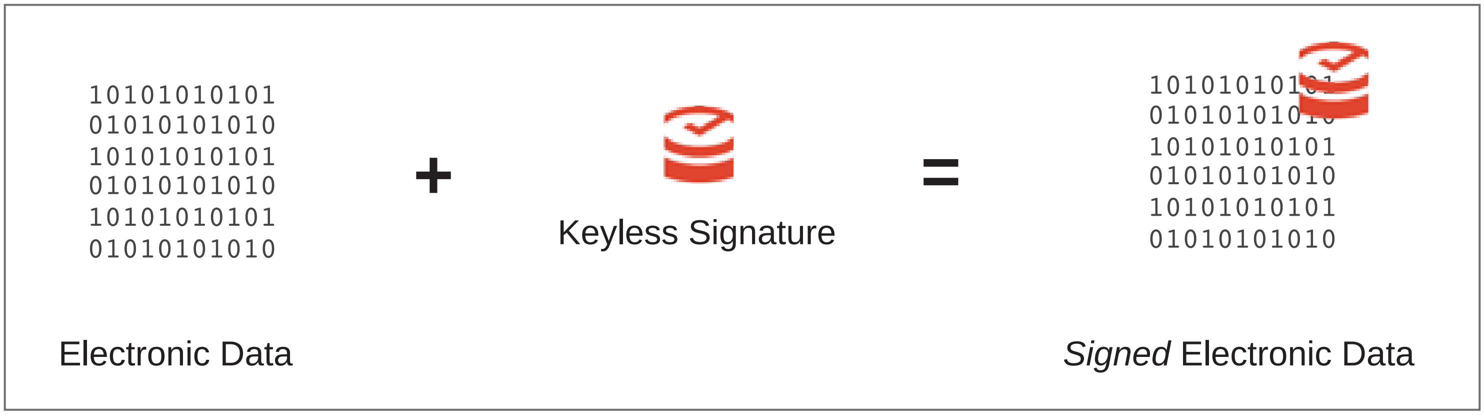
Another important role for data integrity standards will be in the broker risk assessment process. Brokers can include these standards in their risk process to educate their customers and direct them to compliant carriers. One aspect of a data integrity standard is keyless signature infrastructure, known as KSI™.

Keyless signature infrastructure

KSI[1] is a disruptive new technology standard that can effectively address some of the issues insurers face in the rapidly emerging cyber liability domain. It can enable mutual auditability of information systems to allow stakeholders to know the cause of a breach incident, mitigate the risk of breach escalation in real time, and provide indemnification against subrogation and other legal claims.

The concept of a digital signature for electronic data is very straightforward: a cryptographic algorithm is run on the data generating a 'fingerprint of the data,' a tag or Keyless Signature for the data that can then be used at a later date to make certain assertions, such as signing time, signing entity (identity) and data integrity **(Figure 3).**

Figure 3: Keyless signature



KSI offers the first Internet-scale digital signature system for electronic data using only hash-function-based cryptography. The main innovations are:

1. Adding the distributed delivery infrastructure designed for scale
2. No longer requiring cryptographic keys for signature verification
3. Being able to independently verify the properties of any data signed by the technology without trusting the service provider or enterprise that implements the technology

Other features include:

- Unlike digital certificates, keyless signatures never expire, the historical provenance of the signed data is preserved for the lifetime of the data, and people are not required in the signing process.
- Use of Keyless Signatures strengthens legal non-repudiation for data at rest.
- There are no keys to be compromised and/or keys to revoke. This fundamentally changes the security paradigm. It is important to understand that if data integrity relies on secrets like keys or trusted personnel, when these trust anchors are exploited, there becomes an unlimited liability for the data protected by those trust anchors. This occurs because there is no way to determine what has happened to the data signed by those private keys or maintained by those trusted personnel. Evidence can be eliminated, data changes can occur without oversight, and log/event files can be altered. The exploiters can provide the picture they want you to see. Keyless Signatures remedies this problem.

[1] KSI by Guardtime (www.guardtime.com) is based on mathematical proofs and keyless cryptographic functions approved by the EU and the US National Institute of Standards and Technology (NIST). These proofs and functions withstand exploitation even with advances in quantum computing, meaning that digital assets signed by KSI will have proof information retained over the lifetime of the asset.

- During a breach, Active Integrity can be provided with cyber alarms and correlated to other network events by auditors, network operations center and security operations center(s). Active Integrity means real-time, continuous monitoring and verification of data signed with Keyless Signatures. With Active Integrity, real-time understanding is achieved as to the coherence and reliability of technical security controls and whether or not the digital asset has integrity.
- Underwriting cyber policies becomes much simpler and more efficient because there is transparent evidence certifying the integrity of the data, the technical security controls protecting the information, and rules governing the transmission, modification, or state of the insured asset(s).

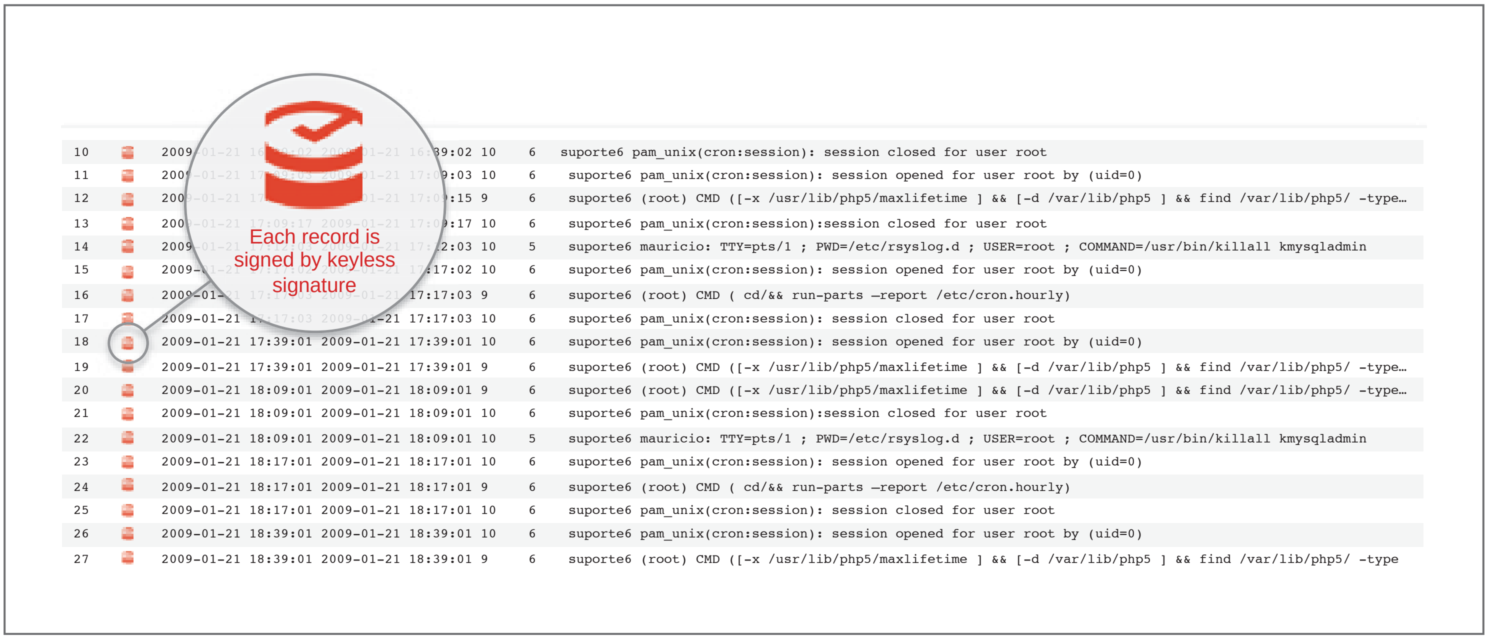
A "Managed Security Service" resulting from the implementation of KSI marks a new era for insurers. As they seek organizational intelligence of digital assets to make real-time policy adjustments, they are also making concrete conclusions about the insured asset risks, threat, exposure and cyber landscapes affecting clients.

Claims processing and disputes become simpler as the technology preserves the forensic traceability and historical provenance of the digital asset, enabling rapid determination of when and how a breach or manipulation occurred and who or what was involved. Hackers and malicious insiders cannot cover their tracks. Moreover, proving negligence is now possible. Negligent acts may be quickly detected and proven in the event the service provider does not comply with the contracts maintained in force with the enterprise.

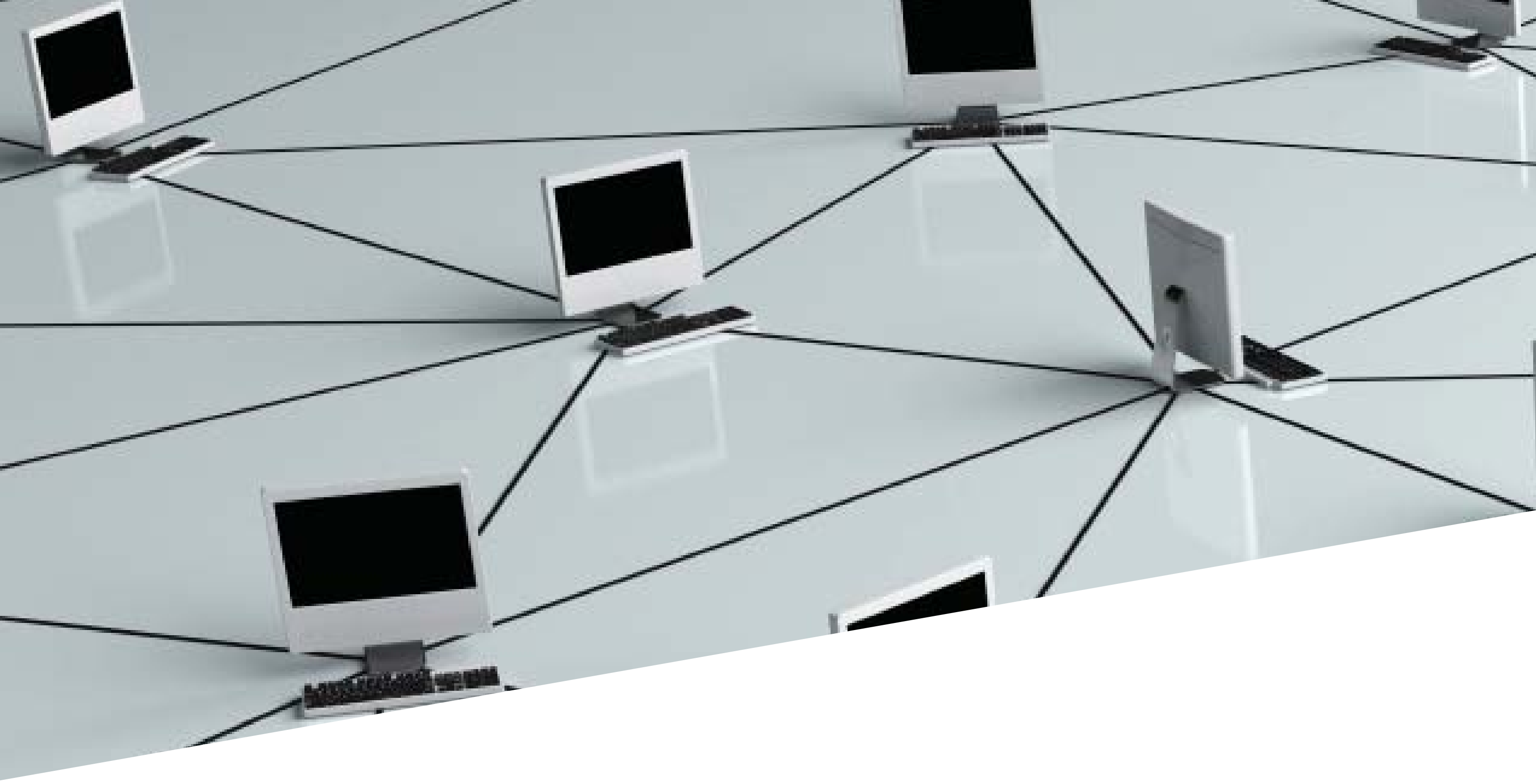
Maintaining data integrity

Most breaches today go unnoticed until long after they occur and the damage has been done. Active integrity involves continuous verification of the integrity of data in storage using keyless signatures. **Figure 4** shows how this works in IT systems logs. It is equivalent to having an alarm on your physical property and a motion detector on every asset that cannot be disabled by insiders.

Figure 4 Example of systems log integration



```
10   2009-01-21 16:39:02 2009-01-21 16:39:02 10   6   suporte6 pam_unix(cron:session): session closed for user root
11   2009-01-21 17:09:03 2009-01-21 17:09:03 10   6    suporte6 pam_unix(cron:session): session opened for user root by (uid=0)
12   2009-01-21 17:09:15 2009-01-21 17:09:15 9    6    suporte6 (root) CMD ([-x /usr/lib/php5/maxlifetime ] && [-d /var/lib/php5 ] && find /var/lib/php5/ -type…
13   2009-01-21 17:09:17 2009-01-21 17:09:17 10   6    suporte6 pam_unix(cron:session):session closed for user root
14   2009-01-21 17:12:03 2009-01-21 17:12:03 10   5    suporte6 mauricio: TTY=pts/1 ; PWD=/etc/rsyslog.d ; USER=root ; COMMAND=/usr/bin/killall kmysqladmin
15   2009-01-21 17:17:02 2009-01-21 17:17:02 10   6    suporte6 pam_unix(cron:session): session opened for user root by (uid=0)
16   2009-01-21 17:17:03 2009-01-21 17:17:03 9    6    suporte6 (root) CMD ( cd/&& run-parts –report /etc/cron.hourly)
17   2009-01-21 17:17:03 2009-01-21 17:17:03 10   6    suporte6 pam_unix(cron:session): session closed for user root
18   2009-01-21 17:39:01 2009-01-21 17:39:01 10   6    suporte6 pam_unix(cron:session): session opened for user root by (uid=0)
19   2009-01-21 17:39:01 2009-01-21 17:39:01 9    6    suporte6 (root) CMD ([-x /usr/lib/php5/maxlifetime ] && [-d /var/lib/php5 ] && find /var/lib/php5/ -type…
20   2009-01-21 18:09:01 2009-01-21 18:09:01 9    6    suporte6 (root) CMD ([-x /usr/lib/php5/maxlifetime ] && [-d /var/lib/php5 ] && find /var/lib/php5/ -type…
21   2009-01-21 18:09:01 2009-01-21 18:09:01 10   6    suporte6 pam_unix(cron:session):session closed for user root
22   2009-01-21 18:09:01 2009-01-21 18:09:01 10   5    suporte6 mauricio: TTY=pts/1 ; PWD=/etc/rsyslog.d ; USER=root ; COMMAND=/usr/bin/killall kmysqladmin
23   2009-01-21 18:17:01 2009-01-21 18:17:01 10   6    suporte6 pam_unix(cron:session): session opened for user root by (uid=0)
24   2009-01-21 18:17:01 2009-01-21 18:17:01 9    6    suporte6 (root) CMD ( cd/&& run-parts –report /etc/cron.hourly)
25   2009-01-21 18:17:01 2009-01-21 18:17:01 10   6    suporte6 pam_unix(cron:session): session closed for user root
26   2009-01-21 18:39:01 2009-01-21 18:39:01 10   6    suporte6 pam_unix(cron:session): session opened for user root by (uid=0)
27   2009-01-21 18:39:01 2009-01-21 18:39:01 9    6    suporte6 (root) CMD ([-x /usr/lib/php5/maxlifetime ] && [-d /var/lib/php5 ] && find /var/lib/php5/ -type
```



Due to the volatile nature of electronic data, any hacker knows how to delete or manipulate logs to cover his/her tracks and attribute his/her activity to an innocent party, which is why attribution of crimes on the internet is so difficult. Integrity is the big gaping security hole. A loss of integrity is what leads to data breaches, introduced by malware, viruses or malicious insiders. Public key infrastructure (PKI) will never be the solution to integrity or usable for large-scale authentication of data at rest.

The forensic evidence of keyless signatures makes legal indemnification issues easy to resolve, highlighting who, what, where and when a digital asset was touched, modified, created or transmitted. This places the onus on the "use" of data and not collection, providing auditability across service providers and the internet. Privacy is maintained, but there is also transparency and accountability for how data is used. Every action can be traced back to the original source that is legally responsible. This simplifies service-level agreements, pinpoints liability in the event of accidental or malicious compromise, and indemnifies independent data providers from legal claims.

Cybersecurity and data privacy are inextricably linked. Indeed, data privacy and confidentiality can be achieved only with effective security. Compromise can be detected and addressed through real-time awareness, incident response, data-loss prevention, investigation and network resilience.

Insurers need to protect the data and IP in their systems and develop strategies to avoid further manipulation and compromise. As EY has learned,from working with clients, negligence and lack of awareness can open the door to risk. More education is needed to develop data protection and detection programs that will enable improvement.

Estonia: NATO headquarters for cybersecurity

Estonia solved the data integrity issue as a country following a disabling cyber attack in 2007. The result was less confidentiality and obfuscation. Instead, there is more irrefutable transparent evidence to independently verify and enable trust in transactions and interactions on their networks. Estonia has applied the same principle for systems. No keys or encryption – just mathematical proof of everything that happened.

By integrating KSI into networks, every component, configuration and digital asset can be tagged, tracked and located with real-time verification – no matter where that asset is transmitted or stored.

With real-time awareness, incident response, data loss prevention, investigation and/or network resilience, it is now possible to detect and react to any misconfiguration, network, component or application failure in the country.

High-performance analytics, or a combination of structured and unstructured data, is changing the ways of the insurance industry after decades of conservatism.

Big data security challenges for insurers

The Industrial Internet, the Internet of Things (IoT), mobile devices, and network connected sensors (such as connected vehicles) are increasingly drivers for change in the digital economy as is the shift to doing business in the cloud. The word ''cloud'' conjures up perceptions of unprotected data and a risk that the data could exist outside the country where it originated. This perception of a lack of security has been a major barrier to mainstream adoption, but that is about to change as data integrity standards for data security and information assurance emerge that will make outsourcing to the cloud more secure than in corporate data centers.

Coping with big data and governance

In the past, large financial risk models have taken days to run, especially when doing risk-scenario simulations. This has held back the ability to get information quickly to the C-suite to make better decisions when they needed most. Running models in the cloud across multiple processors, where the modeling software can process successfully across multiple cores, means large models can now be run in a matter of minutes as opposed to days. Once the model data enters the cloud, the need to prove data integrity is paramount to ensure that the models returning from the cloud are original.

Once the model data enters the cloud, how does one actually trust this data? Machine-to-machine and autonomous sensor data being managed by machines assumes the security protocols and handling of machine-generated data is rock solid and invulnerable to compromise. This is a false premise and, as we have said earlier, this is critically the wrong assumption to make. Machines, their communication protocols, software, rules, and application programming interface (API) exposure will always have flaws. The need to prove data integrity is paramount to ensure that the models returning from the cloud are original.

For example, if perimeter security defense systems and confidential encryption are ultimately compromised, how then can the Industrial Internet and the data lakes it feeds be secured and assured to have integrity? Can they be trusted in a way that ensures the decisions machines are making to tweak and optimize performance are coming from trusted sources and utilizing the right algorithms and rules engines?

To mitigate these attacks, there is only one alternative if you assume compromise and that is real-time, continuous integrity monitoring and tamper detection to make real-time decisions via KSI because KSI:

- Does not rely on confidential certificates or secrets that, if exposed, result in unlimited liability to the enterprise.
- Is digital signature instrumentation at the data level that provides proof of time, identity and authenticity without vulnerable trust anchors like secrets or administrators.
- Scales — to the petabytes, exabytes, and zettabytes of data imagined being generated from Industrial Internet sensors — all autonomously being managed by machines.
- Provides verifiable truth of any connection, configuration or data element from a 'trusted' source.
- Evidence is also portable. The signature can travel with the data or be independently verified regardless of location or status of the network (offline or online).
- Is future-proof. Even in the advent of quantum computing, KSI signatures will remain valid long after current cryptographic algorithms are broken with increasing strides in quantum high-performance computing.

The clouds maintaining these capabilities are a series of big data repositories whose content is a combination of transactions, enterprise data, public data, sensor data from devices and social media data collection; as well as information rules governing the use of the information With KSI, the insurance industry can answer questions that could not have been asked before the advent of big data with governance rules that can be continuously verified.

Integrity of the process

KSI allows companies to manage big data through four dimensions: velocity, variety, volume and veracity. The latter is clearly important and the least understood. IBM puts the cost of poor data quality at over US$3 trillion per year. The correctness of data, infrastructure components and the integrity of the process — spanning collection, ingestion, fusion, correlation/analysis and delivery — are critical to making correct decisions and preventing breaches of data privacy. In today's hostile environments, threats and accidental or malicious incidents that manipulate and processes will certainly lead to incorrect conclusions.

Insurance is the risk industry, and business is based on analyzing good data in order to evaluate, comprehend and mitigate the risks. The advent of new technologies has enabled risk stakeholders in the industry to perform enhanced data analytics to gain more insights into the customer, risk assessment, financial risk management and quantification of operational risk.

Innovate for success

Insurance master databases are one of the biggest sets of data in any sector and are growing exponentially. They are fueled by telematics, social media, unstructured email data and new technologies that analyze data quickly from many sources. Change is needed to keep pace. If the insurance industry does not innovate, it will be commoditized through social networks. So leading insurers are changing their vision to a ''management by data analytics'' approach to customers, risk assessment and financial analysis.

Insurers and reinsurers have always had to cope with incomplete or partial data from their clients, restricting their ability to see or understand the big picture. Analysis consistently assumed that data would be precise and accurate but made assumptions for missing data. Looking forward, the need for these assumptions will become a thing of the past. Insurers will increasingly demand data from their customers and partners to supplement primary data and enhance their analytical results.

Big data offers the opportunity to engage more with predictive modeling and to better forecast choices based on an in-depth statistical analysis across the enterprise.

A wake-up call to re-evaluate and retool analytics

The industry cannot escape the big data challenge or the potential litigation or class action suits that may emerge from the analyses. It is these types of parallel and aggregate risks that could prove the largest threat from huge increases in legal reserving and claims. Agile (re)insurers need to be alert to changing trends within the market and ensure that policy terms and conditions do not leave them exposed.

Wherever there are threats, there are always risks that create opportunities. Telematics is one opportunity in the automotive industry that generates large amounts of data. The changes in sensor and data technology have led to this major new line of business, creating volumes of new data.

Other trends that the industry needs to be aware of:

Big data will undoubtedly reshape the insurance industry and keep it relevant. For years, it had big data but did not know it or use it. The wake-up call is here, and it is time for a critical re-evaluation and re-tooling of analytical capabilities.

It offers the opportunity to engage more with predictive modeling and to better forecast choices based on an in-depth statistical analysis across the enterprise.

Once a tangible is on a balance sheet, data can be mathematically modeled along with other assets and offset against liabilities, and that value can be traded on a data exchange.

The industry will not be querying more data; it will query *all* data. This is different from past data warehousing, the breeding ground for analytics, because it performs analytics on almost any type of data format, including images, videos, monitoring devices, embedded data and social media.

There is no longer a simple one-on-one relationship of server to data storage. Instead, virtualization architecture draws from huge repositories of content and data archives as a single holistic global and enterprise resource.

A glimpse of the future

Insurers face many key issues in security, data integrity and cyber risk. A real and far-reaching opportunity exists to assess how data, an intangible, can be valued as an asset and assessed by organizations, as well as how new advances in data security and data integrity can pave the way for this development. Estimating the value of data and closely aligning its measurement with company strategy can lead to competitive advantage.

We have set out to prove that the new world order is made of intangibles and that data is the next big thing in the intangible space and the glue that links other intangibles together. It is paramount that boardroom thinking and accounting practices align to this new world structure — otherwise, the lack of ownership of the data and the risk of losing that data packaged up as some form of tradable asset without control could lead to a serious bubble, or cyber subprime,[2] where the wrong people manage data for negative effect. Data integrity standards are emerging at the right time to address these concerns and needs for the well-intentioned players.

Steps for insurers to take

From our experience serving our clients, we note that companies are mandating self-assessments or commissioning independent external assessments of information security measures. Overall, information security functions are improving to more effectively meet business needs and create value for the organization. There is still much to do to keep pace with the volume and frequency of cyber threats, which continue to be one of the most important risks facing the insurance industry today.

EY believes that insurance companies should maintain the triad of confidentiality, integrity and availability of information systems and data. To improve in these areas of information security, they need to:

- Develop and implement a long-term, enterprise-wide security program that addresses processes, controls, organization and governance, as well as reporting, metrics, privacy and data protection
- Invest in cybersecurity and do a better job of articulating and demonstrating the value of that investment to stakeholders
- Establish a framework of continuous improvement in analytics and reporting, people, processes, and technology
- Design and execute solutions to measure, monitor and report on the effectiveness of the security program
- Refine strategies based on changing threats, risks and business imperatives

[2] "Risk Nexus: Beyond data breaches: global interconnections of cyber risk," Zurich and Atlantic Council, 2014.

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

EYG no: EG0198
1407-1283151
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com

Our two-part series addresses some important cybersecurity issues for insurers to consider. Both papers highlight the need for companies to reach beyond what they have done in the past and to develop effective data and risk programs that will protect their businesses from cyber threats in the future. Cyber insurance, security and data integrity and Mitigating cyber risk for insurers are available at www.ey.com/insurance.