IONICA

Security and Compliance

In 2020 alone, over 2,953 security breaches were publicly announced by the third quarter. Over 36 billion records were exposed due to these breaches *(source)*. The true figures are likely far higher.

Cyber security threats and who that perpetrate them are more sophisticated than ever. Today, the most significant and damaging attacks are orchestrated by highly organised criminal groups and nation states. Their targets range from government and military departments, hospitals and health organisations, energy and civil infrastructure, to technology service providers and software companies. Even private individuals of interest and those connected to or in close proximity to them are at risk. No longer can managers credibly claim that there is no reason for them to be targeted – if anyone ever could. Quite literally, everyone is now a target.

Below is a break-down of publicly identified security incidents by industry.

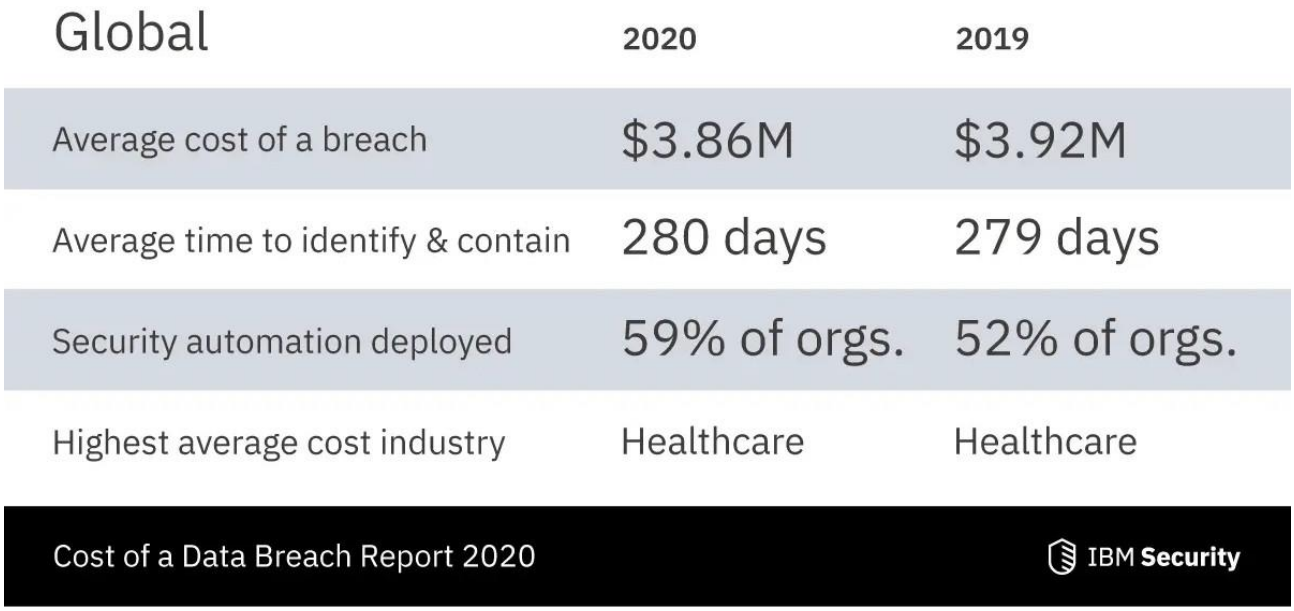
Incidents	Total	Small (1-1,000)	Large (1,000+)	Unknown	Breaches	Total	Small (1-1,000)	Large (1,000+)	Unknown
Total	29,207	1,037	819	27,351		5,258	263	307	4,688
Accommodation (72)	69	4	7	58		40	4	7	29
Administrative (56)	353	8	10	335		19	6	7	6
Agriculture (11)	31	1	0	30		16	1	0	15
Construction (23)	57	3	3	51		30	3	2	25
Education (61)	1,332	22	19	1,291		344	17	13	314
Entertainment (71)	7,065	6	1	7,058		109	6	1	102
Finance (52)	721	32	34	655		467	26	14	427
Healthcare (62)	655	45	31	579		472	32	19	421
Information (51)	2,935	44	27	2,864		381	35	21	325
Management (55)	8	0	0	8		1	0	0	1
Manufacturing (31-33)	585	20	35	530		270	13	27	230
Mining (21)	498	3	5	490		335	2	3	330
Other Services (81)	194	3	2	189		67	3	0	64
Professional (54)	1,892	793	516	583		630	76	121	433
Public (92)	3,236	22	65	3,149		885	13	30	842
Real Estate (53)	100	5	3	92		44	5	3	36
Retail (44-45)	725	12	27	686		165	10	19	136
Wholesale Trade (42)	80	4	10	66		28	4	7	17
Transportation (48-49)	212	4	17	191		67	3	8	56
Utilities (22)	48	1	2	45		20	1	2	17
Unknown	8,411	5	5	8,401		868	3	3	862
Total	29,207	1,037	819	27,351		5,258	263	307	4,688

Table 4. - Number of security incidents and breaches by victim industry and organization size

Source: Verizon Data Breach Investigations Report, 2021

Costs of security breaches

At an average cost for a single breach of $3.86M, the financial consequences of a cyber security breach can be staggering – data loss, enormous brand damage, and potential legal liability are also major risks. A security incident is also often a massive disruption to business operations, taking focus away from organisation strategy.



Source: IBM

Such widespread and sophisticated threats require comprehensive, strong, and continuously adaptable defences. IONICA's business-focused analytical approach delivers the protection and the firepower to keep your data, your customers, and your business safe.

Types of cyber attack

The large variety of attack types fall into key categories – denial of service *(DoS)*, web application (*HTTP-based*) attacks *(those that are typically carried out through a web browser or client)*, social engineering *(those that happen by coercing or tricking people into enabling or facilitating an incident)*, system intrusion *(where a computer or other system is cracked into)*, lost and stolen assets *(where physical computers, or media like drives, discs, tapes, or paper documents are stolen)*, miscellaneous errors *(like configuration errors or other mishaps)*, and everything else.

The following chart depicts a break-down of the types of cyber attack *incident* that took place during 2020. These attacks did not necessarily perpetrate a breach of defences in all cases, but likely caused disruptions in business operations, harm to systems or users, and/or brand damage.

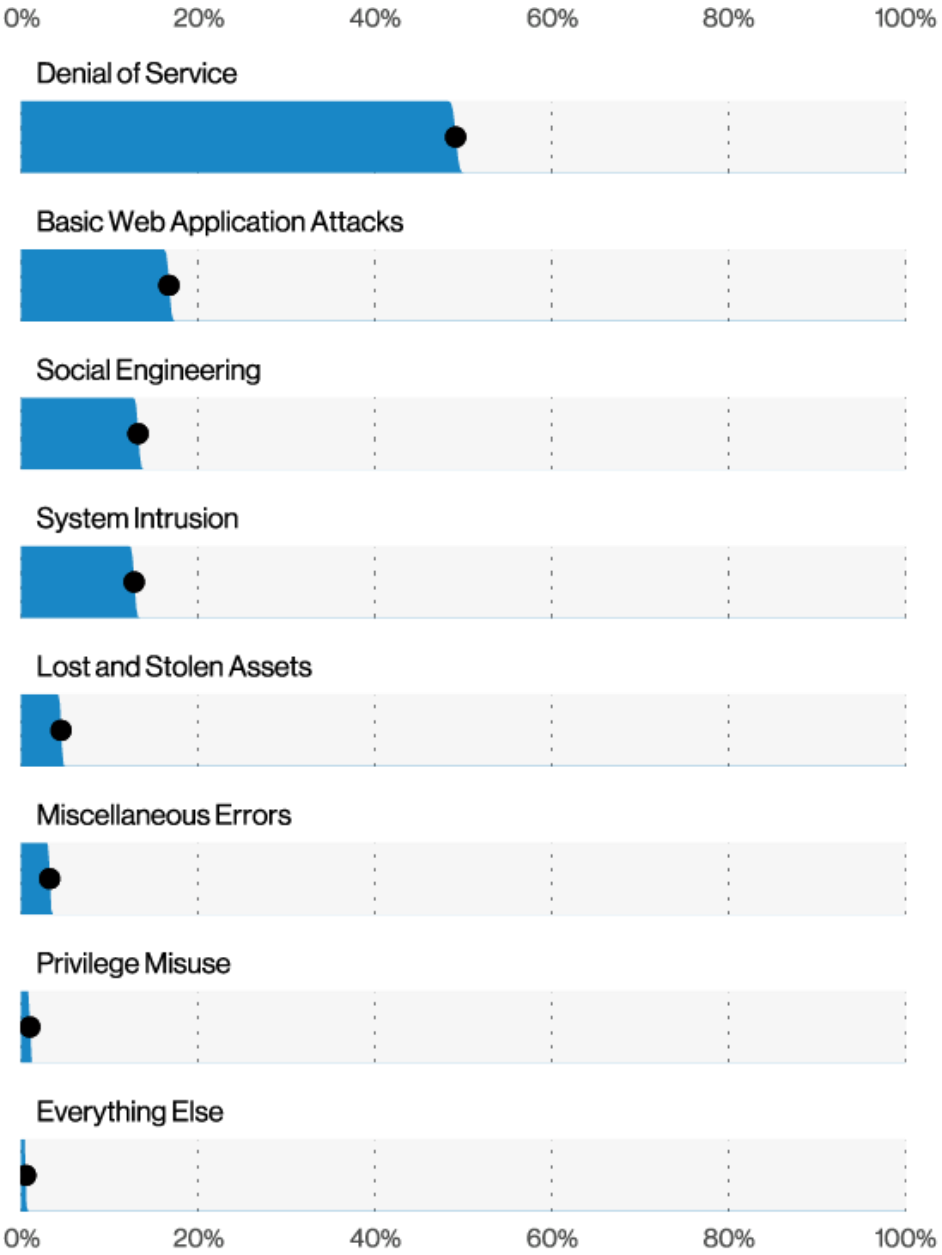


Figure 6. Patterns in incidents (n=29,206)

Source: Verizon Data Breach Investigations Report, 2021

The following chart depicts a break-down of security breaches that took place in 2020.

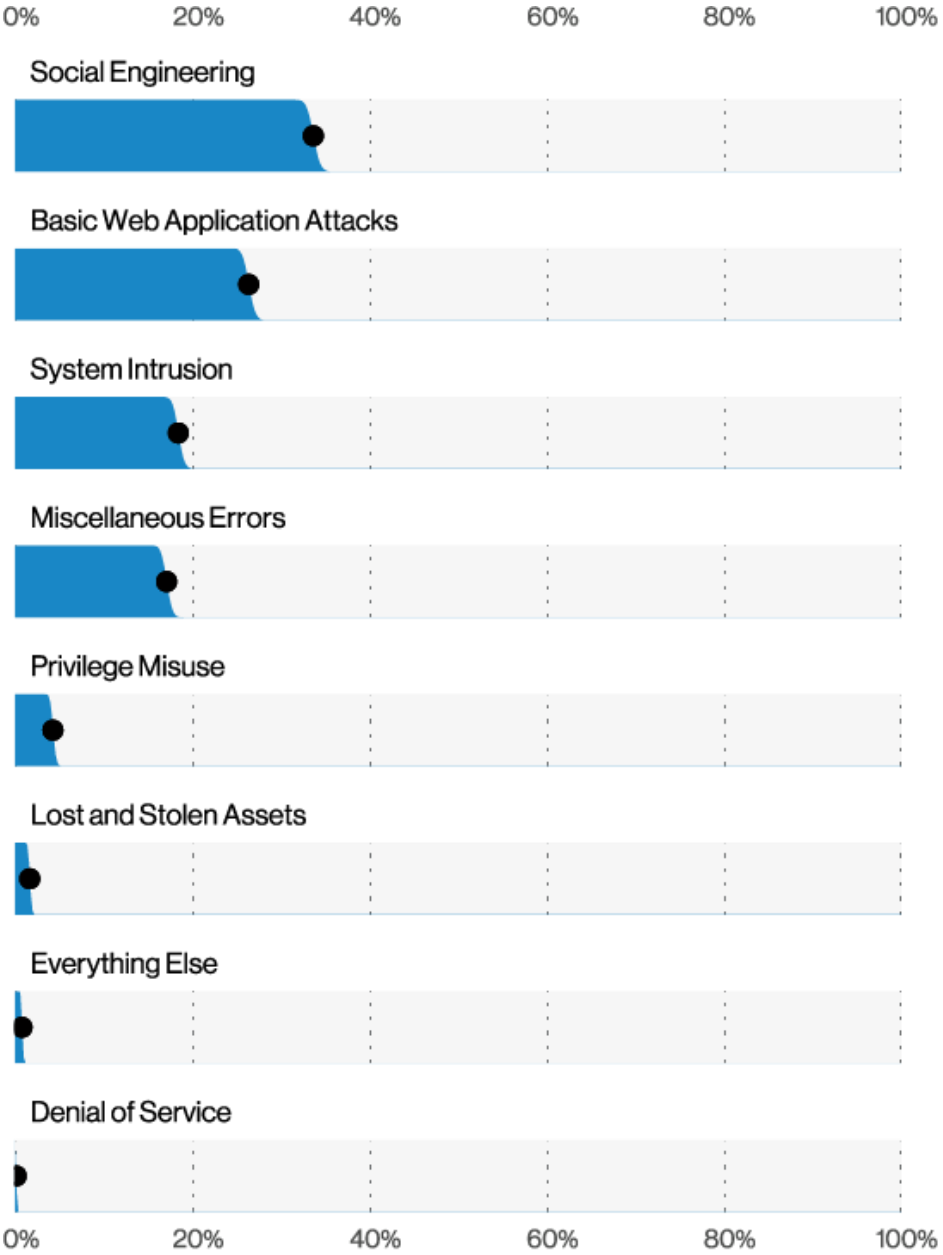


Figure 5. Patterns in breaches (n=5,275)

Source: Verizon Data Breach Investigations Report, 2021

Perpetrators

One of the most common questions we hear from clients when another major breach or threat is identified in the news is, “who would bother doing this?”

The truth is more straightforward than it may seem. In the early days of the computing and the Internet, it was often believed that computer hackers were young people working out of their parents’ basements – causing mischief out of boredom or curiosity. The real perpetrators of the largest and most damaging attacks – as well as of many smaller attacks – are often employed by or affiliated with criminal gangs or nation-states. Their motivations are most often financial. While corporate and national security espionage drives a relatively smaller number of officially recorded attacks and breaches, attacks carried out for the purposes of espionage are often the most damaging and wide-reaching *(affecting large amounts of data and/or large numbers of organisations or people)*. Interestingly, state-sponsored actors regularly carry out financially motivated attacks as well as espionage-related attacks, as described in Verizon’s data breach investigations report: *“However, since 2015 it is relatively common for state-sponsored actors to also crave that cold hard cash as the financial motives for those actors have fluctuated between 6% and 16% of recorded breaches.”*

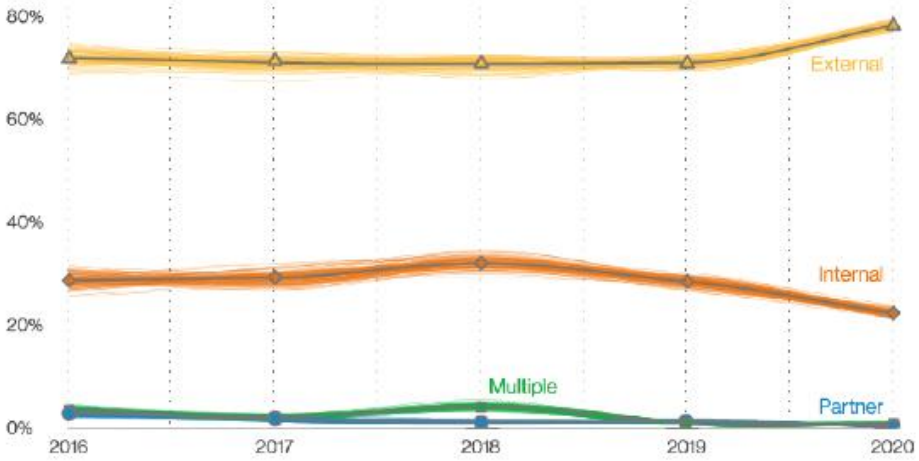


Figure 14. Threat actor over time in breaches

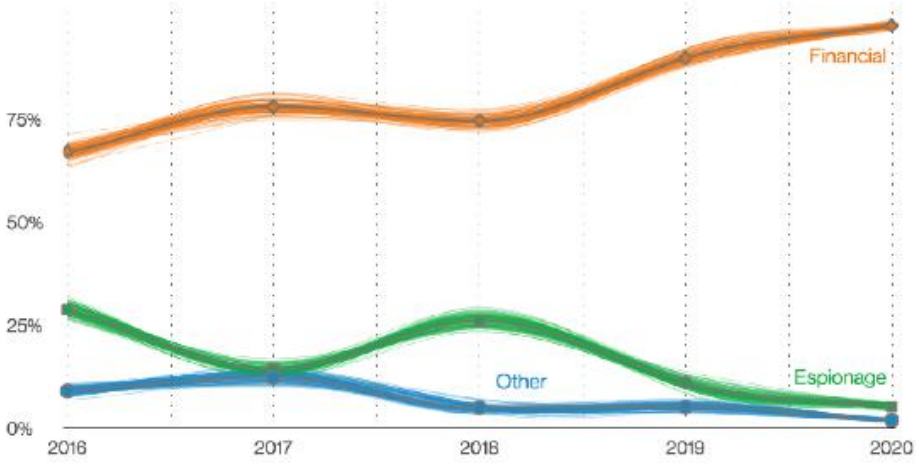


Figure 15. Top threat actor motive over time in breaches

As in past years, financially motivated attacks continue to be the most common (Figure 15), likewise, actors categorized as Organized crime continue to be number one (Figure 16).

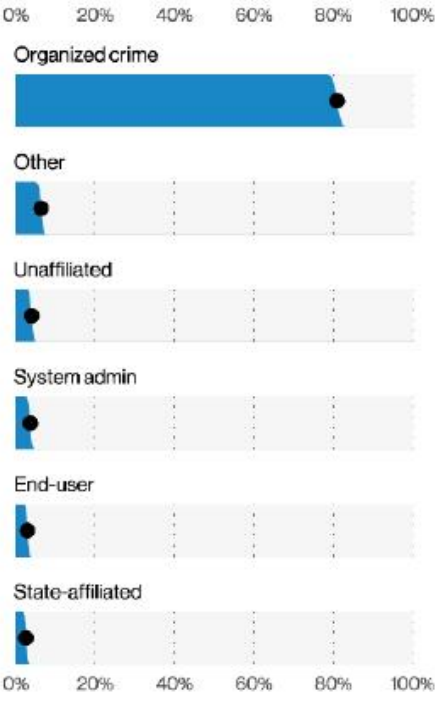


Figure 16. Top threat actor varieties in breaches (n=2,277)

Source: Verizon Data Breach Investigations Report, 2021

Security vs. compliance

Cyber security, generally, is the pursuit of protecting the organisation's people, assets, data, and operations in the digital realm.

Compliance is generally conformity to specific standards and/or laws governing digital activities, operations, communications, and data storage.

So, a "secure" technology or technology environment is not necessarily compliant with any particular standard, and a technology or environment that meets standards is not necessarily secure *(or secure enough for a particular situation or use case)*.

How security and compliance keep your business safe

Their deficiencies notwithstanding, cyber security standards are developed with security in mind, or as a central aim. In this way, they can help your organisation become more secure and accountable.

Cyber security practises are essential in protecting organisational data, assets, operations, employees, and customers. For example, encryption protects communications from eavesdropping and data from unauthorised access and theft. Protocols and controls for handling e-mail attachments and links, for installing software, and for controlling office and data centre access are all measures to protect against malware and ransomware attacks.

Key security standards

Among the few widely accepted global security standards, PCI-DSS *(payment card industry data security standard)* stands out as the most prominent. PCI-DSS was developed by banks and credit card companies to ensure the integrity of credit card transactions online and in real space.

Key national or regional standards include SoX and HIPAA in the United States; PIPEDA, PHIPA, and CyberSecure Canada in Canada, and GDPR in the European Union.

All of these standards contribute to better security for organisations and improved safety and privacy for individuals.

Protecting your organisation from cyber security threats

The scale and prevalence of security threats can seem overwhelming, and nearly impossible to counter. The good news, however, is that a secure environment that maintains efficiency and operational effectiveness certainly is possible. In fact, it may be less effortful and more affordable than you think.

Key protection mechanisms include:

- Keep systems and applications up to date.
- Ensure proper configuration of systems, applications, Internet-connected services, firewalls, and network equipment.
- Implement a web application security firewall.
- Implement denial of service network firewall rules, and DoS mitigation tools on load balancers and/or web servers.
- Ensure custom applications and web sites are developed according to secure coding practises.
- Utilise encryption for data at rest (*files and data stored on computers or removable media*), data in transit, and all communications *(e-mail, chat, voice and video conferencing)*.
- Ensure vendors *(software and SaaS providers, cloud platforms, video conferencing and telecommunications providers)* conform to secure practises.
- Formulate internal and external security auditing plans, which evaluate security actions and controls.
- Set up monitoring for security incidents, with host and network-based intrusion detection systems. Such systems report on potential security incidents, and notify staff when suspected serious incidents occur.
- Create comprehensive security incident response plans, which describe how the organisation will respond to any security incidents that may occur. Include a review schedule to ensure the plans are updated regularly to address new threats.

While there are never guarantees that security practise *(or anything at all)* will completely prevent any or all incidents, a truly comprehensive and adaptable approach that includes measures like these would certainly make any organisation a much more challenging target, and would deflect the vast majority of attacks.

Highly trained cyber security experts are available to deliver all of the above, and to integrate them into your current technology environments.

Given the likelihood and risks of security incidents today, and the opportunities presented to prevent them, the time to bolster cyber security is now. Then, the digital world can be a safer place for all of us.