BUSINESS PERCEPTION OF IT SECURITY: IN THE FACE OF AN INEVITABLE COMPROMISE

IT Security Risks Report 2016 for North America
Kaspersky Lab

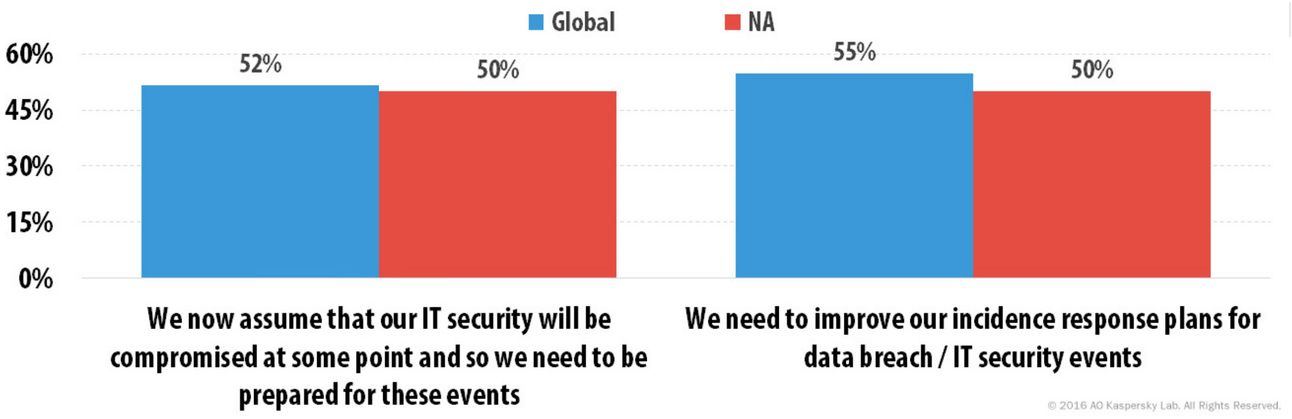
CONTENT

INTRODUCTION

Evaluation of the business threat landscape can be broken down into two major areas: financial and technical. The former we covered extensively in our previous report, by measuring security budgets and recovery costs from typical threats. The next step is to take a closer look at real incidents that businesses have to deal with, and measures they take to prevent them.

To investigate cyber threat landscape perception and reality, Kaspersky Lab together with B2B International conducted a global study of more than 4,000 business representatives from 25 countries. We asked businesses about their perceptions of the main security threats they face and the measures used to combat them. This report provides survey insights specific for the North American region.

One of the major findings of this year's research is based about the perception of the threat landscape in general. Companies unanimously state that cyber threats are highly damaging and that cybersecurity is one of the top requirements for business to stay afloat. But attitudes towards general protection approaches are, simply put, rather mixed, as seen in the table below.



Source: IT Security Risks Report 2016, data for North American region

The cybersecurity industry almost unanimously agrees that a working protection strategy should take into account the inevitability of a compromise. Yes, prevention measures like endpoint security, firewalls, and anti-spam systems are still a requirement. But should a breach happen despite all precautions, tools, experts and intelligence should be prepared to act, in order to reduce the damage.

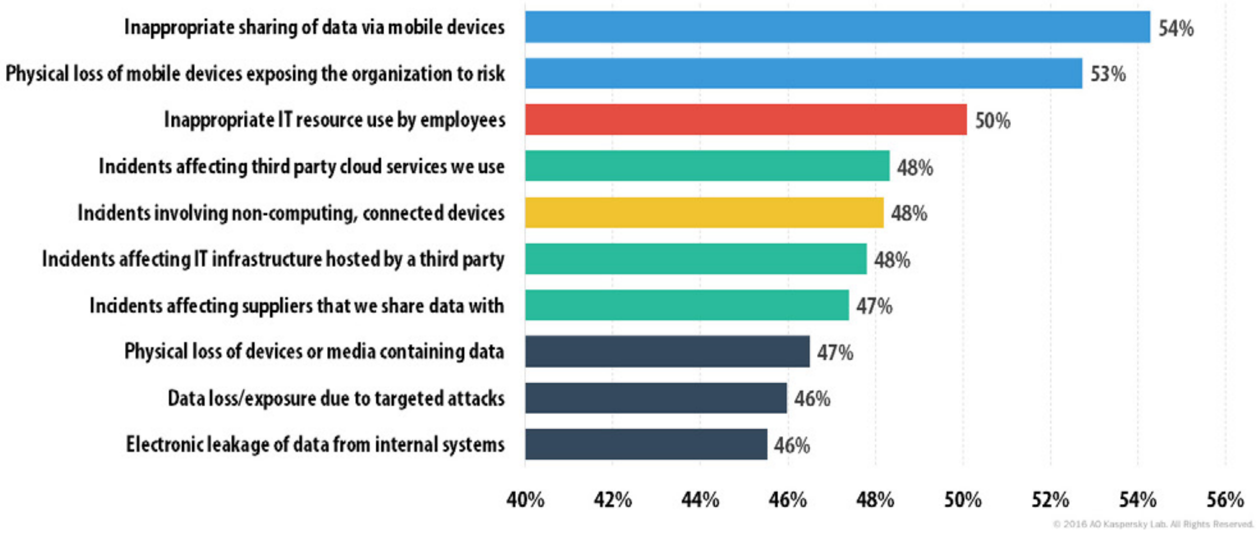
Not all customers agree with this, as our findings show. Only half (**52%**) recognize the need to be better prepared for a security compromise globally, **50%** agree with this statement in North America. We also note the higher share of enterprises identifying the need to improve incidence response, thanks to their generally better research of the threat landscape.

PERCEPTION OF IT SECURITY THREATS

This year, we chose a new approach when asking companies about cybersecurity incidents. Although, we covered some specific threats, we shifted our attention from attack types to damage caused. This allowed us to speak the same language with technical experts as well as business decision-makers.

So how do businesses perceive IT security threats?

Most vulnerable areas of expertise



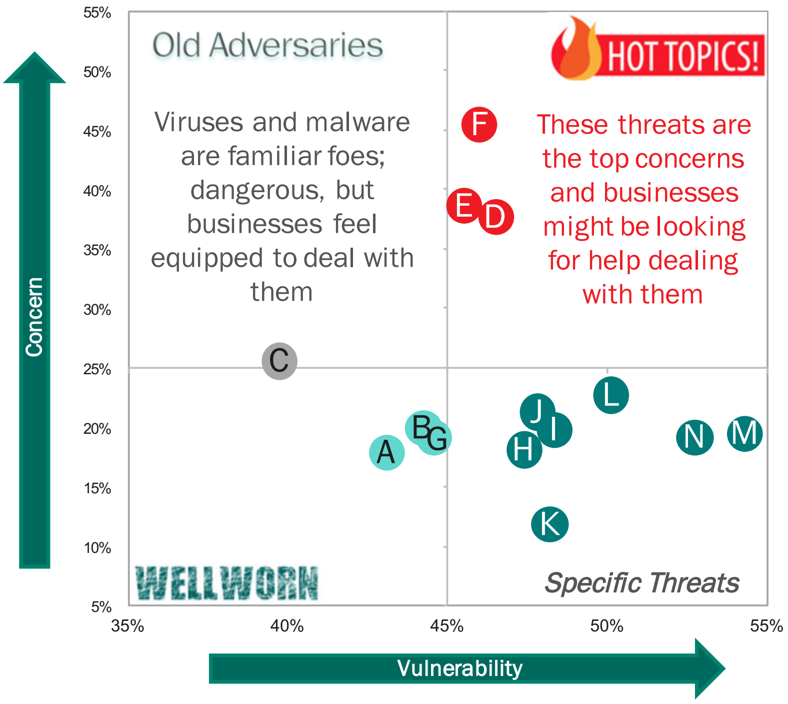
Source: IT Security Risks Report 2016, global data

Six out of ten typical vulnerable areas are directly related to a fear of data loss. But the real surprise is that the most frequent point of vulnerability is inappropriate usage or sharing data via mobile devices, with **54%** of businesses reporting that they face challenges understanding how to address this threat globally, **52%** in North America.

A closer look at mobility: the current business blind spot

Let's take a closer look at the threat of attacks via mobile devices. Businesses are reporting that the number of smartphones and tablets in their organizations is growing rapidly. **37%** of businesses globally report a significant increase in smartphones that access corporate data and have to be managed in different ways, including security. The infrastructure of North American businesses shows more maturity, but **32%** of businesses still reported a significant increase in the number of smartphones. The growing complexity of IT infrastructure is a general concern that is also driving the costs of maintenance and security up. **40%** of businesses admit that IT infrastructure complexity directly affects their ability to maintain the required level of security. In North America the most frequent reason to invest more in IT security is business expansion (**45%**).

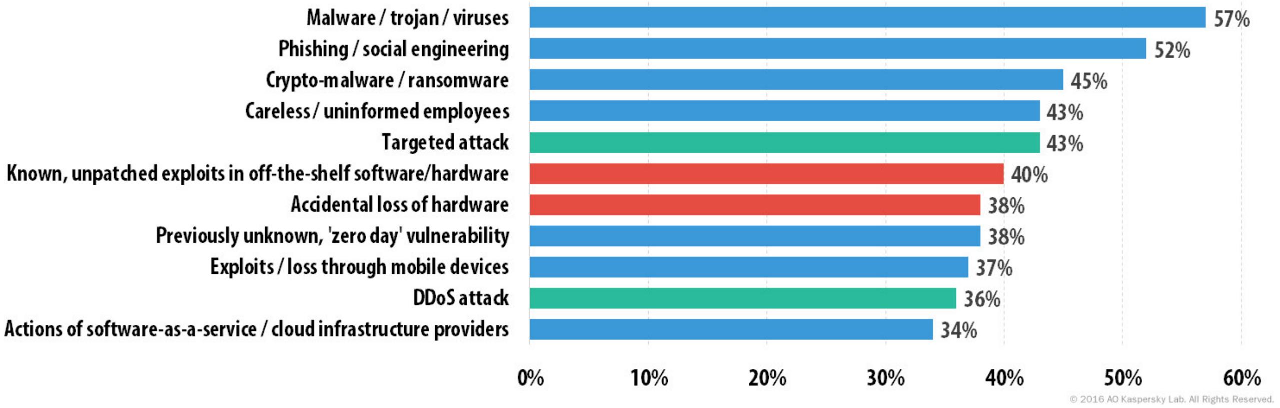
And the problem is more complex than just BYOD. We have seen a significant share of businesses reporting a growth in any type of devices, even virtual servers and desktops. In terms of security the source of the devices does not really matter. What matters is having a proper protection strategy in place. With more than half the company representatives surveyed saying they see trouble in protecting data on mobile devices, this can be identified as the most alarming blind spot of business security today. In the future the scope of protection will likely expand to virtual instances and IoT devices, although many businesses already report these technologies as troublesome for security.



A	Loss of access to customer-facing services
B	Loss of access to internal services
C	Viruses & malware causing a loss of productivity
D	Physical loss of devices or media containing data
E	Electronic leakage of data from internal systems
F	Data loss/exposure due to targeted attacks
G	Data loss/exposure due to attacks on point-of-sale (POS) systems
H	Incidents affecting suppliers that we share data with
I	Incidents affecting third party cloud services we use
J	Incidents affecting IT infrastructure hosted by a third party
K	Incidents involving non-computing, connected devices
L	Inappropriate IT resource use by employees
M	Inappropriate sharing of data via mobile devices
N	Physical loss of mobile devices exposing the organization to risk

Source: IT Security Risks Report 2016, global data

As we see in the graph above, almost all types of consequences are in the high risk zone: from data loss to third-party suppliers, cloud services, IoT and mobile device troubles. One particular area worth noting is targeted attacks: businesses are both highly concerned and feel vulnerable here. It's also interesting to note that, in terms of perception, companies feel they are well protected from malware attacks which cause of loss of productivity. But clearly it's too early to write off the threat of general malware attacks.



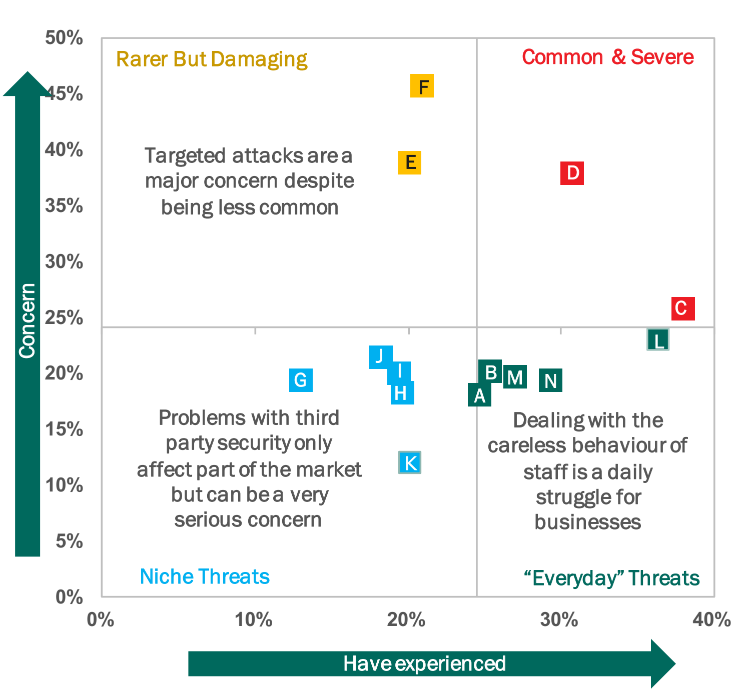
Source: IT Security Risks Report 2016, data for North American region

In this list of actual threats that concern businesses the most, we see old acquaintances such as DDoS and unpatched vulnerabilities in popular software, as well as new arrivals, such as encrypting ransomware. Phishing often becomes the root-cause for different security incidents, and 52% of North American businesses report that this is one of their major concerns.

THE REALITY OF THE THREAT ENVIRONMENT

Looking how perception compares with reality gives us a different breakdown of cyber threats and once again shows that the threat of malware attacks is still prevalent due to the fact that businesses have experienced this more than any other threat.

Concerns vs. Experience



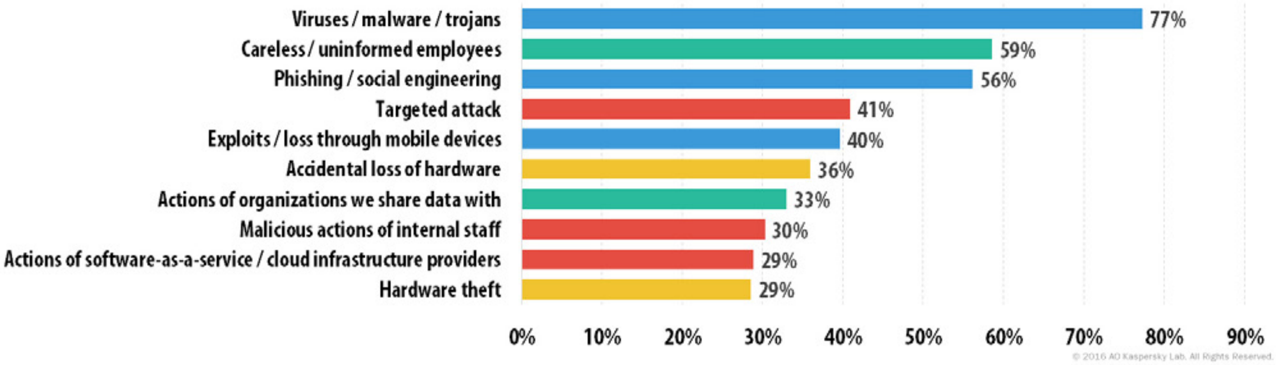
A	Loss of access to customer-facing services
B	Loss of access to internal services
C	Viruses & malware causing a loss of productivity
D	Physical loss of devices or media containing data
E	Electronic leakage of data from internal systems
F	Data loss/exposure due to targeted attacks
G	Data loss/exposure due to attacks on POS
H	Incidents affecting suppliers that we share data with
I	Incidents affecting third party cloud services we use
J	Incidents affecting IT Infrastructure hosted buy a third party
K	Incidents involving non-computing, connected devices
L	Inappropriate IT resource use by employees
M	Inappropriate sharing of data via mobile devices
N	Physical loss of mobile devices exposing the organization to risk

Source: IT Security Risks Report 2016, global data

As illustrated above, the most dangerous threat related to data protection is physical loss and theft of media, which concerns businesses and occurs often. Other related threats like electronic leakage of data from internal systems are worth thinking about, but businesses question the ROI efficiency of relevant efforts.

Fortunately, the emerging threats related to the use of third-party services and infrastructure are comparatively rare, and today can be considered 'niche threats'. And when it comes to the prediction of future threats, cloud, IaaS and IoT challenges are definitely contenders for the next big headache.

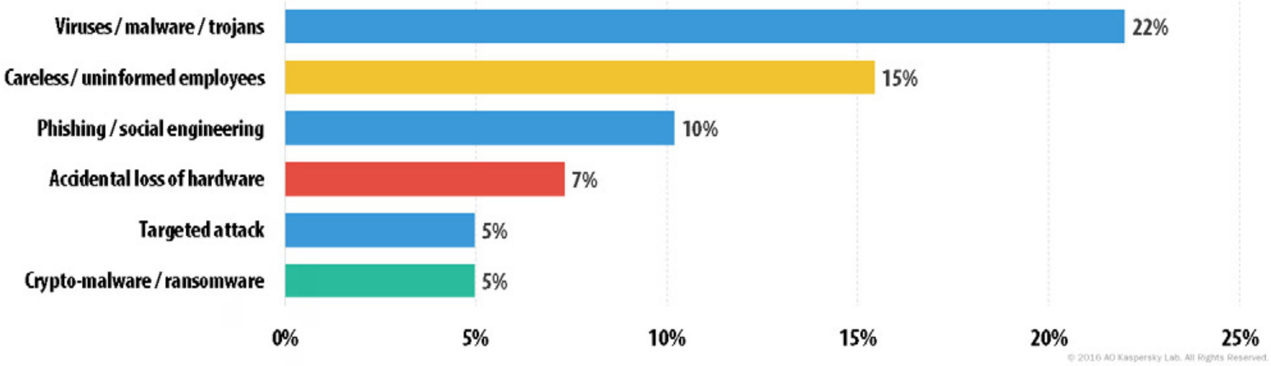
Widespread attack vectors



Source: IT Security Risks Report 2016, data for North American region

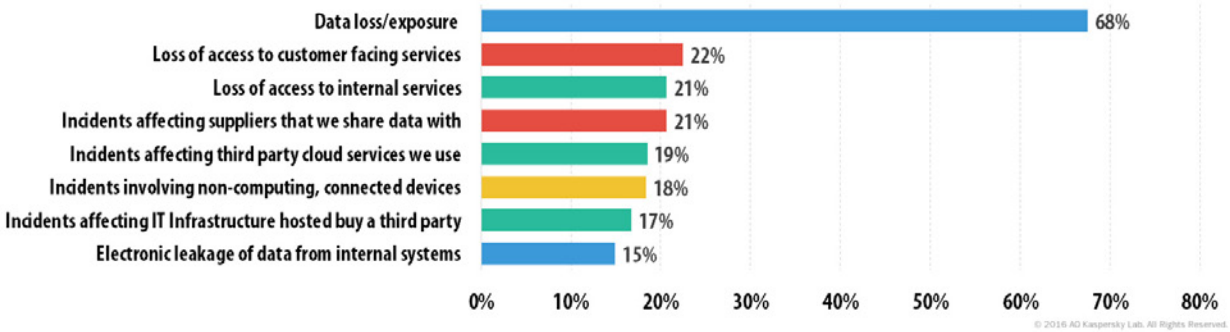
Comparison of 'most feared threats' and actual incident experience highlights the potential areas where businesses have lower visibility. Again, we see the difficulties in managing the security of mobile devices, but the biggest eye-openers are careless employee actions (**59%** of businesses in the North American region report that this contributed to a successful attack).

Top causes: most costly data breaches



Source: IT Security Risks Report 2016, data for North American region

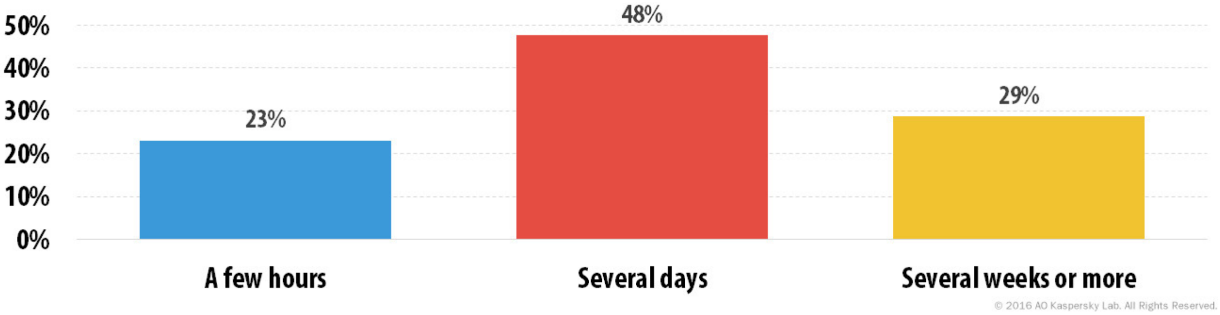
SPECIFIC THREATS: TARGETED ATTACKS



Source: IT Security Risks Report 2016, global data

Here the perception and reality match well, with the most typical consequences of a targeted attack being data loss or theft. The most typical causes that contributed to a successful targeted security breach globally are third-party compromise (**46%** reported this attack vector), exploitation of mobile devices (48%), hacktivist actions (**37%**) and malicious actions of internal staff (**38%**).

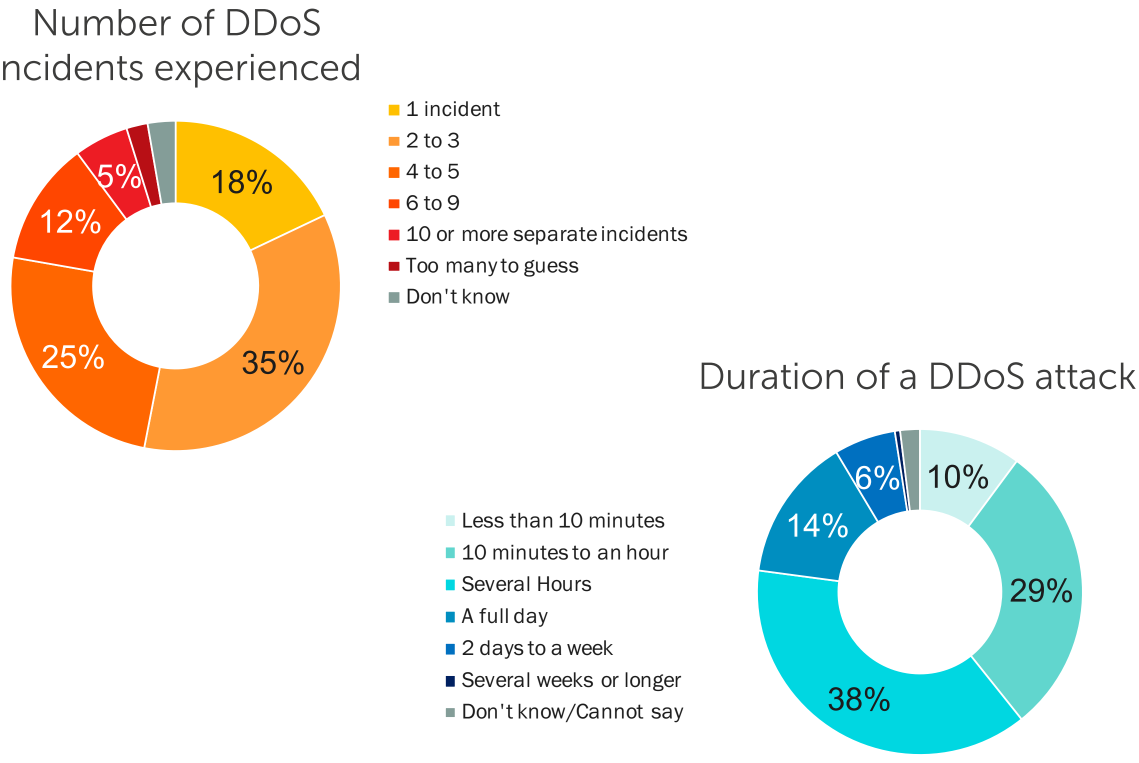
SPECIFIC THREATS: ENCRYPTING RANSOMWARE



Source: IT Security Risks Report 2016, global data

Encrypting ransomware was covered in detail in this IT Security Risks report. The most significant finding is that in three-quarters of all incidents businesses suffer the consequences for quite a long time, with days or even weeks required to recover affected data. Overall, 20% of businessesworldwide reported a serious incident involving ransomware, **17%** in North America.

SPECIFIC THREATS: DDOS ATTACKS



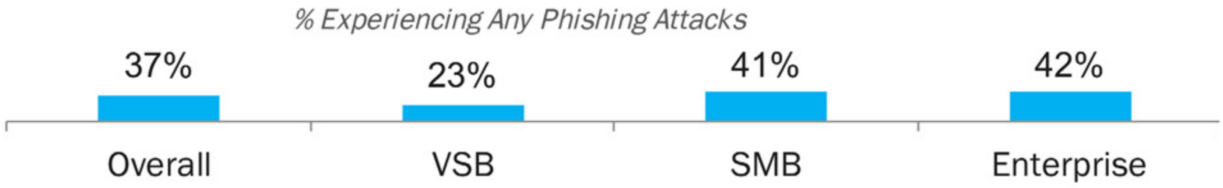
Number of DDoS incidents experienced

Duration of a DDoS attack

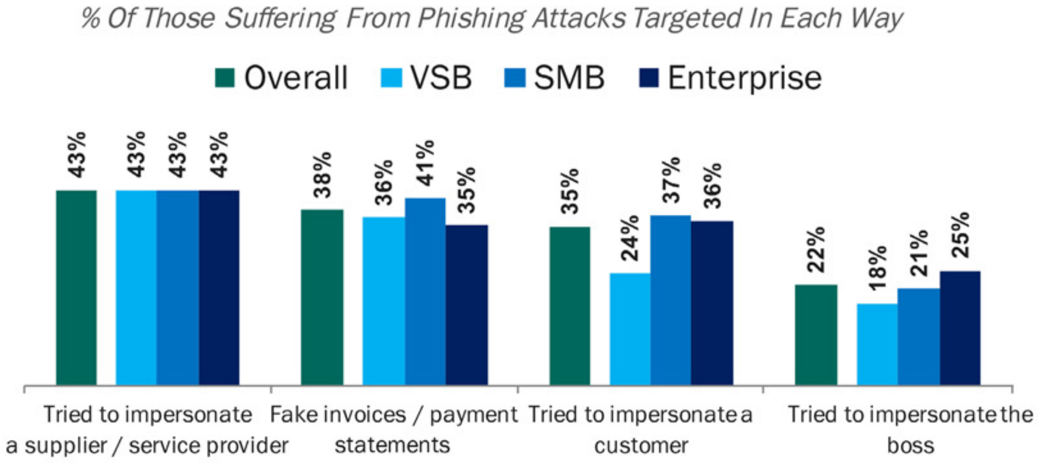
Source: IT Security Risks Report 2016, global data

We found that **17%** of businesses had suffered from a DDoS attack, **12%** in the North American Region. It is also important to note that, for the second year in a row, we observe how DDoS attacks coincide with other types of security breach, particularly a targeted attack. A third (**32%**) of those reporting a targeted attack mentioned DDoS as a likely contribution.

SPECIFIC THREATS: PHISHING



% Experiencing Any Phishing Attacks

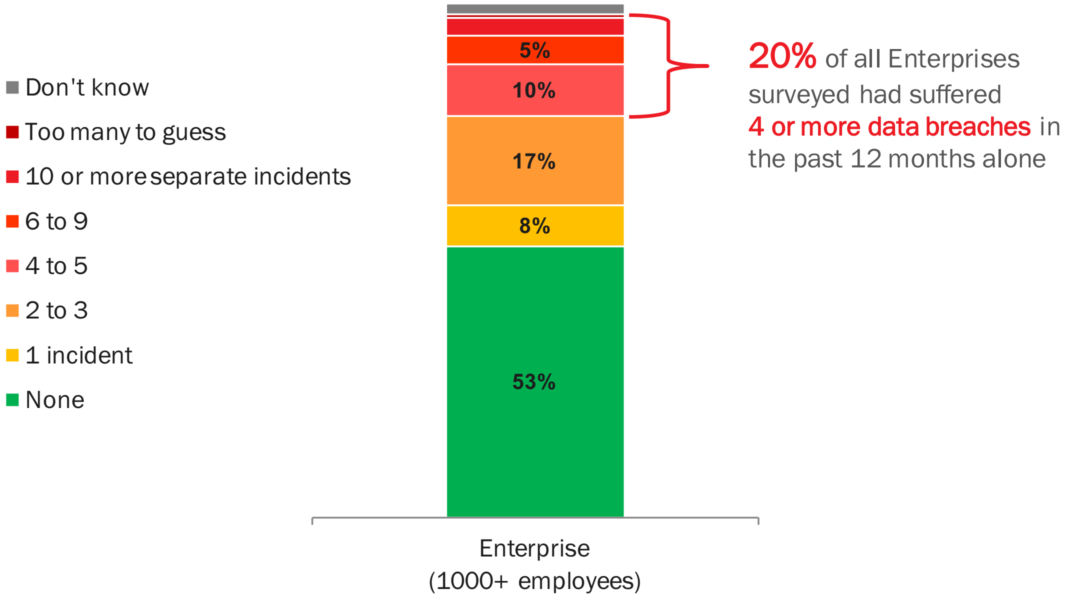


% Of Those Suffering From Phishing Attacks Targeted In Each Way

Source: IT Security Risks Report 2016, global data

Given the perceived and practical importance of protection from phishing, we asked businesses to provide more details on this type of attack. We found that the most frequent type of impersonation used by attackers is pretending to be a third-party supplier or service provider. Overall, **38%** of NA businesses experienced at least one phishing attack.

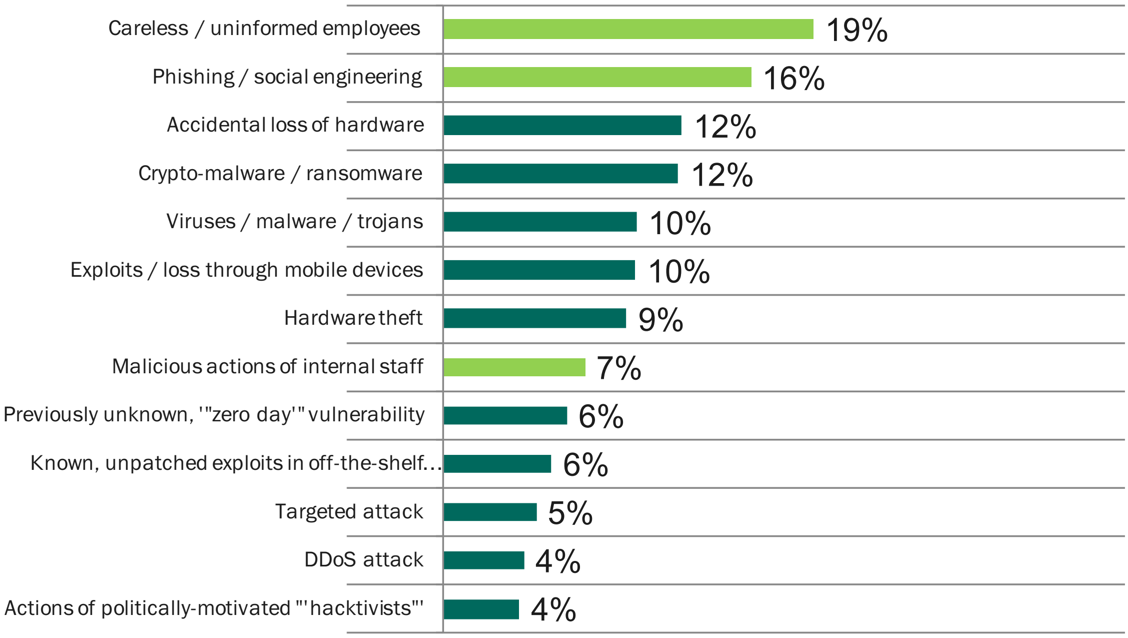
THE CONSEQUENCES



Source: IT Security Risks Report 2016, global data

Overall, our research revealed that **32%** of businesses experienced data loss due to a cybersecurity incident, significantly lower than worldwide (**43%**). Very small companies with up to 50 employees traditionally suffer less from data leakage and more from loss of continuity, but for SMBs and Enterprises data loss is the inevitable consequence of roughly every second attack. **44%** of enterprises in North America suffered four or more data breaches in the past 12 months alone. This is significantly higher than worldwide average, which is just **20%** as shown in the chart above.

Top causes of data leakage: untrained employees, phishing, device loss



Source: IT Security Risks Report 2016, global data

One of the main reasons for data loss or theft is careless employees. Nearly one in five (**19%**) businesses report that this has contributed to a serious data breach. In North America this is also a major contributing factor, with **14%** of businesses citing employee carelessness as a reason for a major data breach.

The key finding of our survey of threat reality is the sheer multitude of threats facing companies, from viruses and phishing to zero-day vulnerability exploitation and DDoS attacks. This threat landscape shows the importance of traditional measures like endpoint anti-malware protection, anti-phishing and vulnerability assessment. But threats like targeted attacks, exploitation of mobile devices and ransomware also call for new approaches.

CONCLUSION: CONNECTING THE DOTS

The security industry finds itself at the point when traditional solutions do not cover some new threats and businesses are still uncertain about 'beyond-prevention' methods like staff training, security audits and consulting. These new methods of protection are strikingly different from the old ones, and may initially seem a bit more difficult to deploy and measure results.

So what's the right approach?

We are confident that 99% of security threats can be repelled by highly-efficient, automated, intelligent software technologies. The remaining one percent requires not technology, but a new mind set.

The success of the next leading security vendor depends on packaging intelligence on the wide variety of cyber threats and protection methods in the most efficient way. Speaking the same language with businesses becomes a necessity of paramount importance.

At Kaspersky Lab we feel that being a trusted advisor is the top priority. Technology is important, but in this report we have shown that the way companies feel about security may be different from how they protect themselves. Protection strategies can sometimes leave out certain important threat areas.

The goal of the true next-generation security is, therefore, joining the areas of perception, threat reality and approach to protection so that they become perfectly aligned. In an ideal world businesses see actual threats attacking them, interpret this data accurately and build defenses to prevent and predict future attacks according to this precise threat model.

Securelist, the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy