

Riadenie rizík informačnej bezpečnosti

Pavol Adamec, PricewaterhouseCoopers Slovensko

eFOCUS

Risk management

- **Risk Identification**

- Assets identification
- Threats identification
- Vulnerabilities identification
- Consequences identification
- Identification of existing Controls

- **Risk Estimation**

- Assessment of Consequences
- Assessment of Likelihood

- **Risk Evaluation**

- Acceptable level of risks

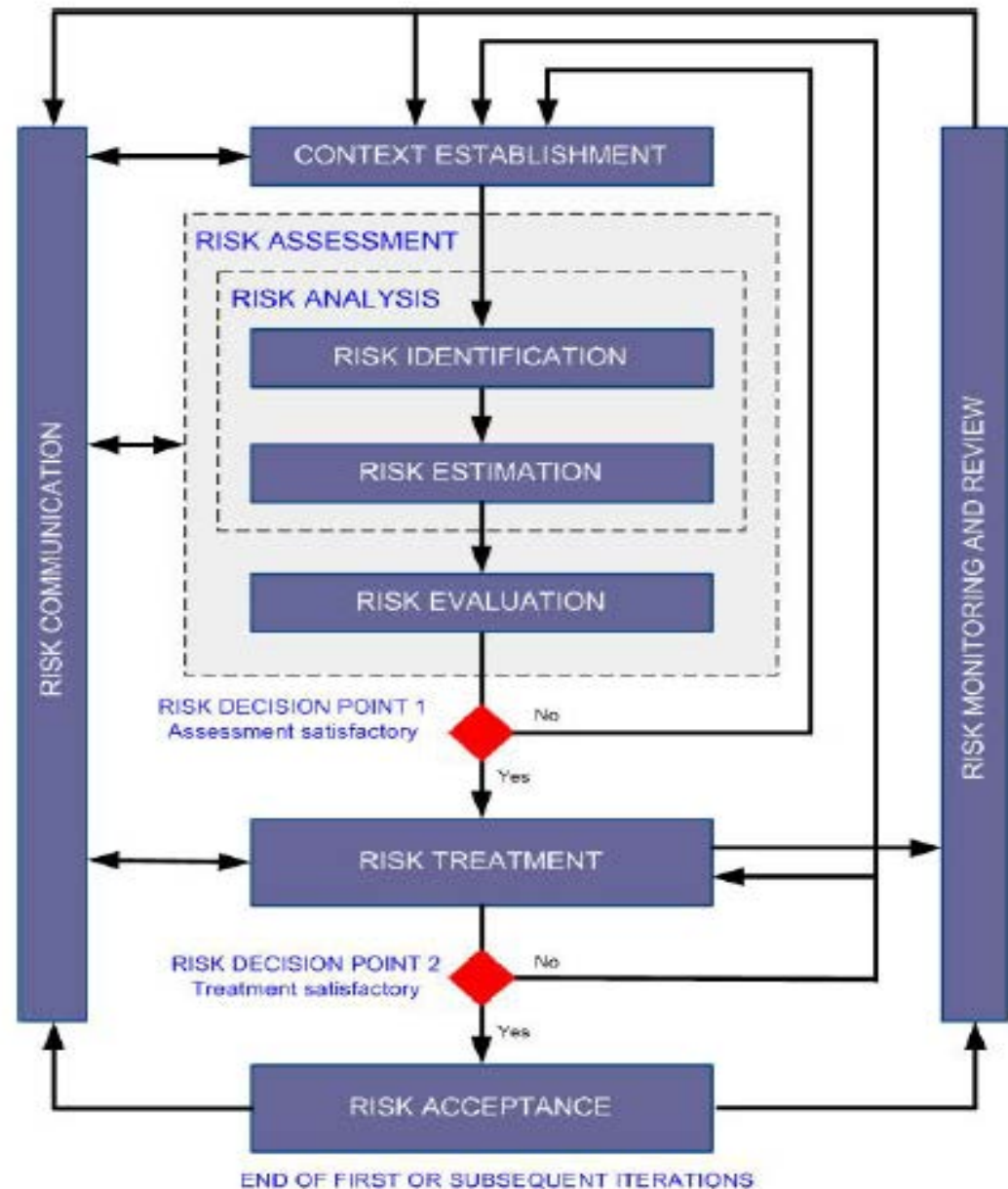
- **Risk Treatment**

- Risk Reduction
- Risk Retention
- Risk Avoidance
- Risk Transfer

- **Risk Acceptance**

- Residual Risks

- **Risk Monitoring and Communication**



Risk Estimation – Areas of Consequences (Impacts)

Possible areas of consequences to defined assets:

- *Personal Safety*
- *Personal Information*
- *Legal and Regulatory Obligations*
- *Law Enforcement*
- *Commercial and Economic Interests*
- *Financial Loss/Disruption to Activities*
- *Public Order*
- *Management and Business Operations*
- *Loss of Goodwill*

Risk Estimation – Examples of Consequences (Impacts)

Severity Level	Financial loss / Disruption of Activities	Personal Information	Legal and Regulatory Obligations
6	The organisation will go out of business	A breach in a legal, regulatory or ethical requirement or publicised intention on the protection of information, leading to serious embarrassment to a group of individuals	No entry
5	Result in losses of more than € 10.000.000	Leading to serious embarrassment to an individual	Enforcement notice, civil suit or criminal offence resulting in unlimited damages/penalty, or a prison term in excess of two years
4	Result in losses of between € 1.000.001 and € 10.000.000	Leading to significant embarrassment to an individual or minor embarrassment to a group of individuals	Enforcement notice, civil suit or criminal offence resulting in damages/penalty of between € 10.001 and € 50.000, or a prison term of up to two years
3	Result in losses of between € 100.001 and € 1.000.000	Leading to minor embarrassment to an individual	Enforcement notice, civil suit or criminal offence resulting in damages/penalty of between € 2.001 and € 10,000
2	Result in losses of between € 10.001 and € 100.000	Distress to an individual (anger, frustration, disappointment) but no breach of legal or regulatory requirement occurs	Enforcement notice, civil suit or criminal offence resulting in damages/penalty of € 2.000 or less
1	Result in losses of € 10.000 or less	Minor distress to an individual but no breach of legal or regulatory requirement occurs	No entry

Likelihood of Occurrence – Example of Definition

Definition	Probability of Occurrence
Frequent	More than once a year
Probable	Once a year
Occasional	Once in 2-3 years
Remote	Once in 5 years
Improbable	Less than once in 5 years

Risk Estimation and Risk Evaluation

Severity Level	Likelihood of Occurrence				
	Frequent	Probable	Occasional	Remote	Improbable
6					
5					
4					
3					
2					
1					

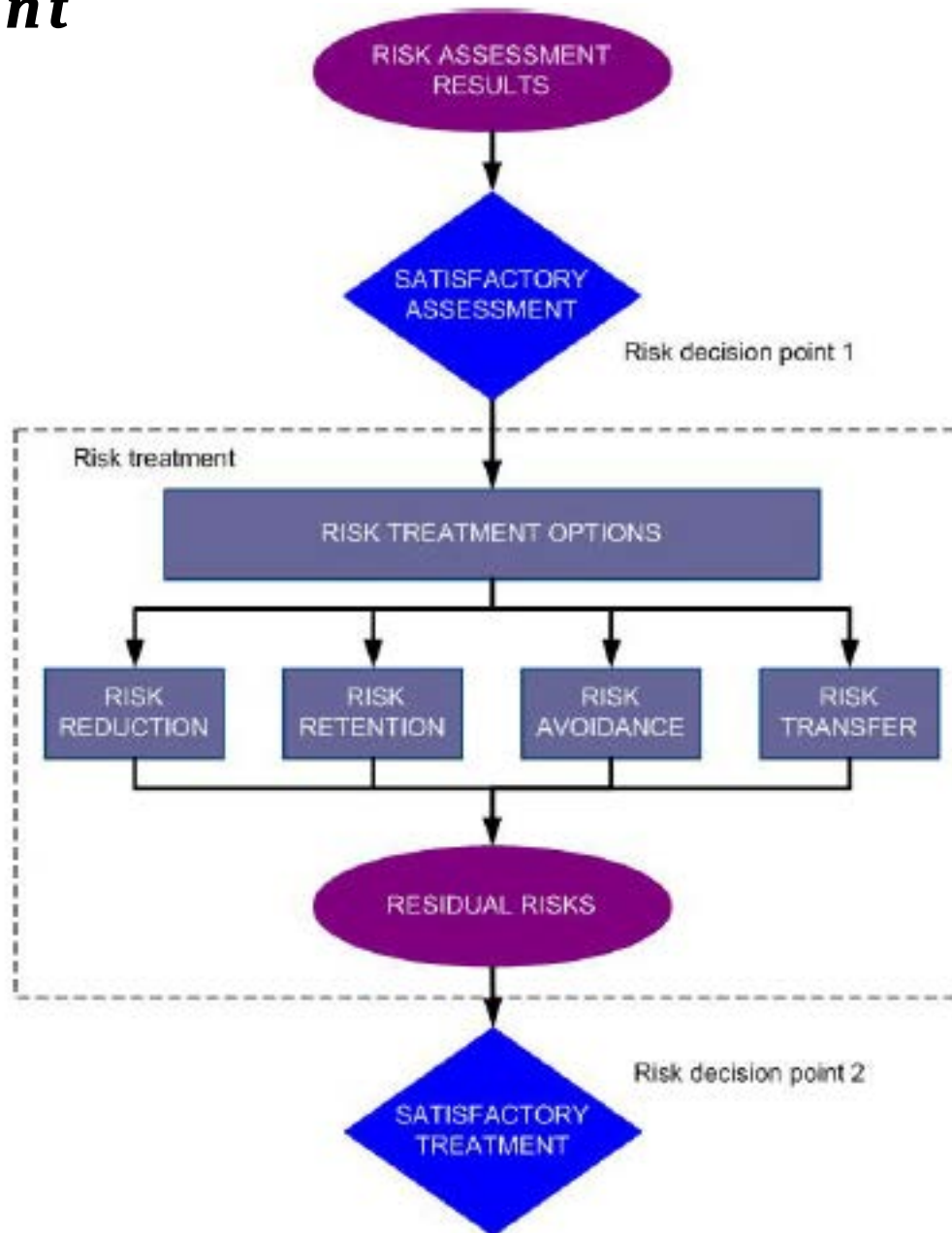
Risk Appetite – the acceptable level of risk

	<i>Risk should be avoided or counter measures implemented as soon as possible</i>
	<i>Undesirable risk, counter measures should be implemented in a reasonable amount of time</i>
	<i>Acceptable risk, existing counter measures are likely adequate. Management review required.</i>
	<i>Acceptable risk, existing counter measures are adequate. Management review not required.</i>

Risk Catalogue

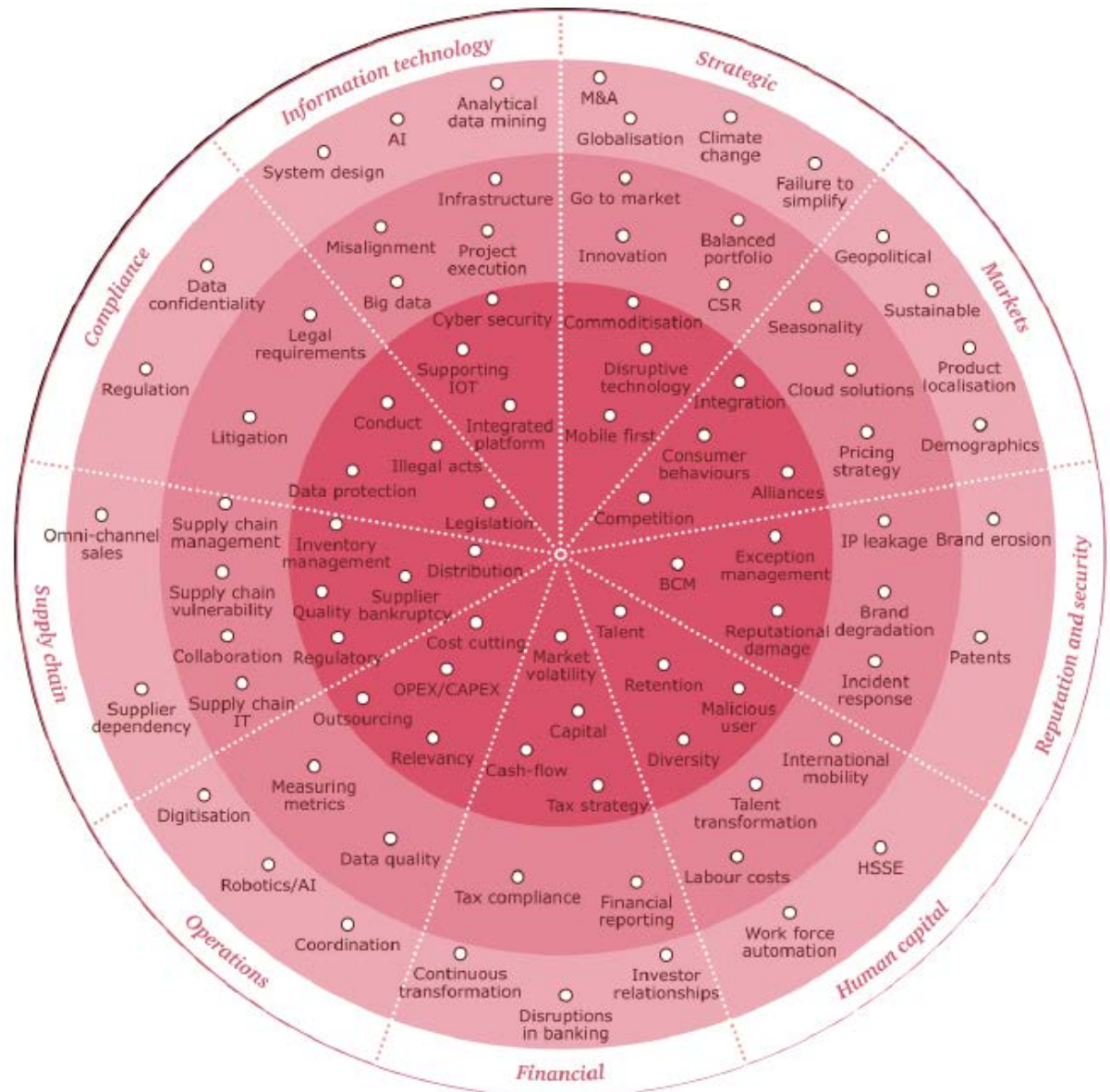
Risk no.	Severity	Likelihood of Occurrence	Risk level	Risk treatment
Risk #1	6	Probable		
Risk #2	4	Frequent		
Risk #3	2	Frequent		
Risk #4	4	Occasional		
Risk #5	6	Remote		
Risk #6	2	Probable		
Risk #7	1	Frequent		
Risk #8	5	Improbable		
Risk #n	1	Remote		

Risk Treatment



Risk Identification – PwC Risk Radar

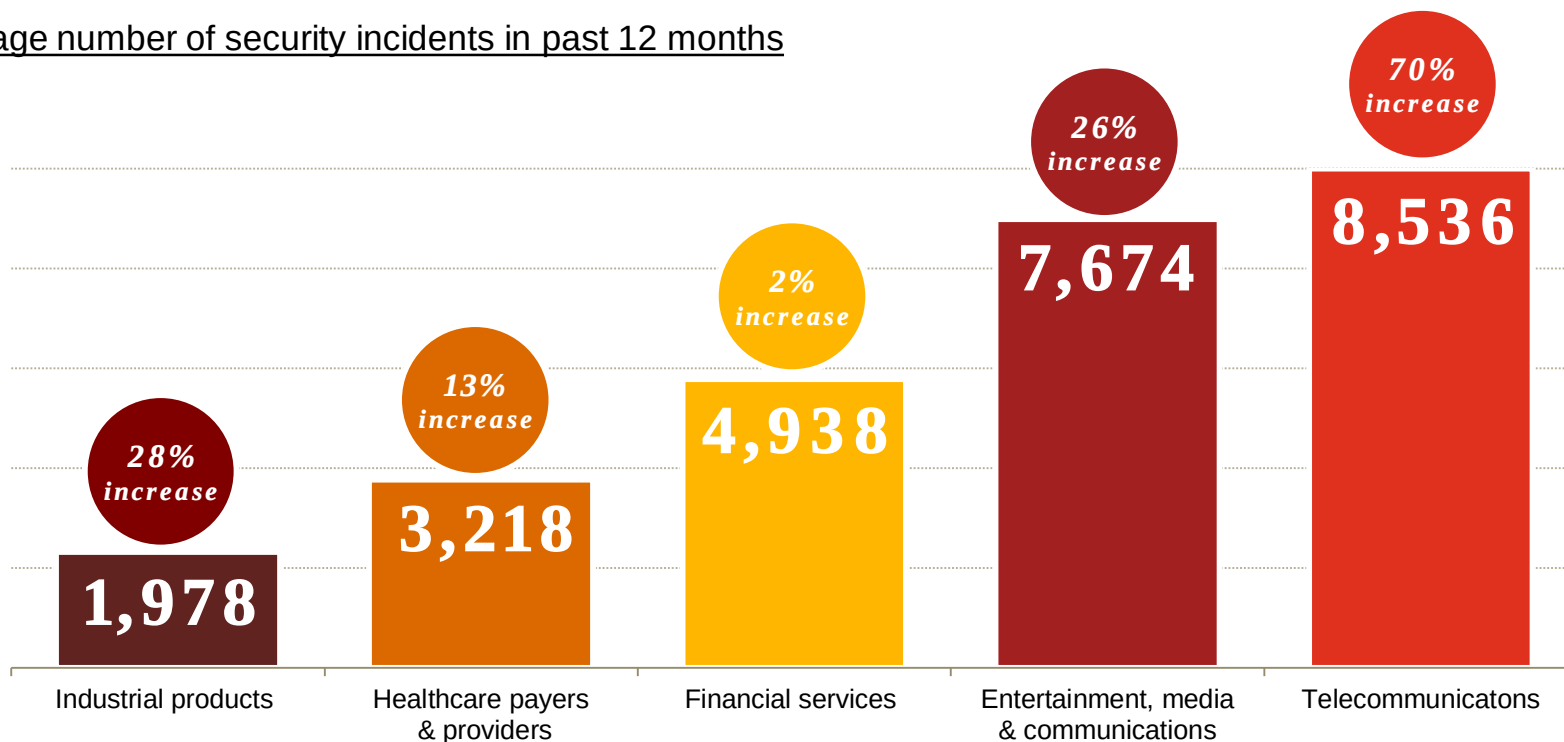
- The creation of “**Risk Universe**”.
- An **interactive tool** developed by PwC Risk Assurance Services department.
- Helps to create a **risk profile** of clients using a broad knowledge and experience **in the specific industry sector**.



In 2016, global respondents detected fewer information security incidents.*

But in five industries, incidents increased over the year before. Several are highly regulated industries that have continuously invested in security, while others are catching up.

Average number of security incidents in past 12 months



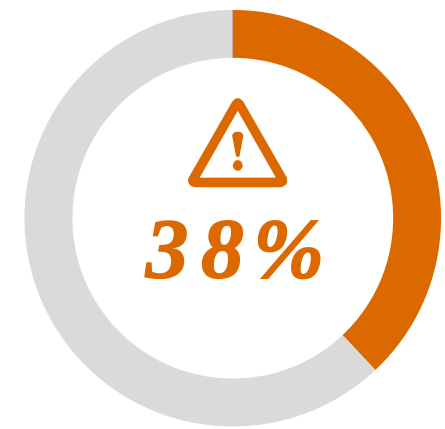
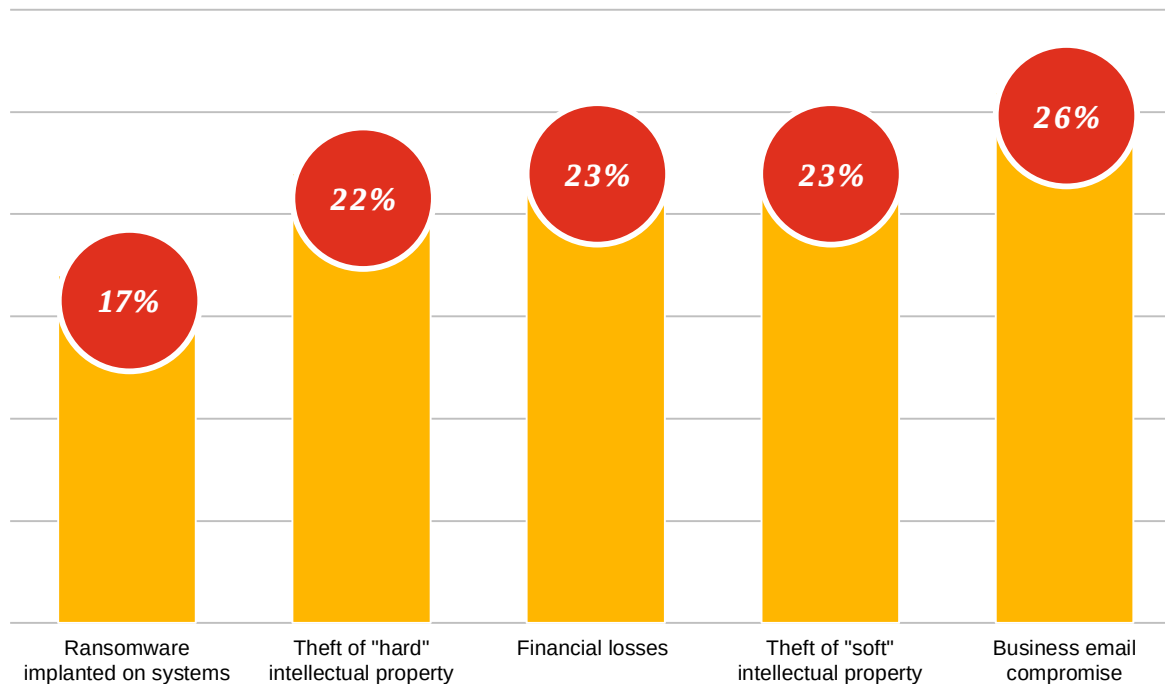
* A security incident is defined as any adverse incident that threatens some aspect of computer security.

Question 18: "What is the number of security incidents detected in the past 12 months?"

Business email compromise and ransomware emerge as growing business impacts, while phishing is the top vector.

Respondents cite business email compromise as the leading impact of incidents, while phishing becomes the top vector of cybersecurity incidents.

Business impacts of security incidents



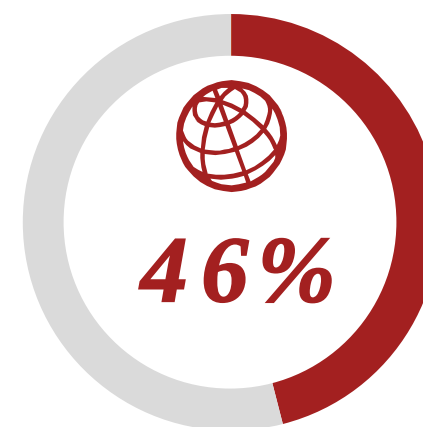
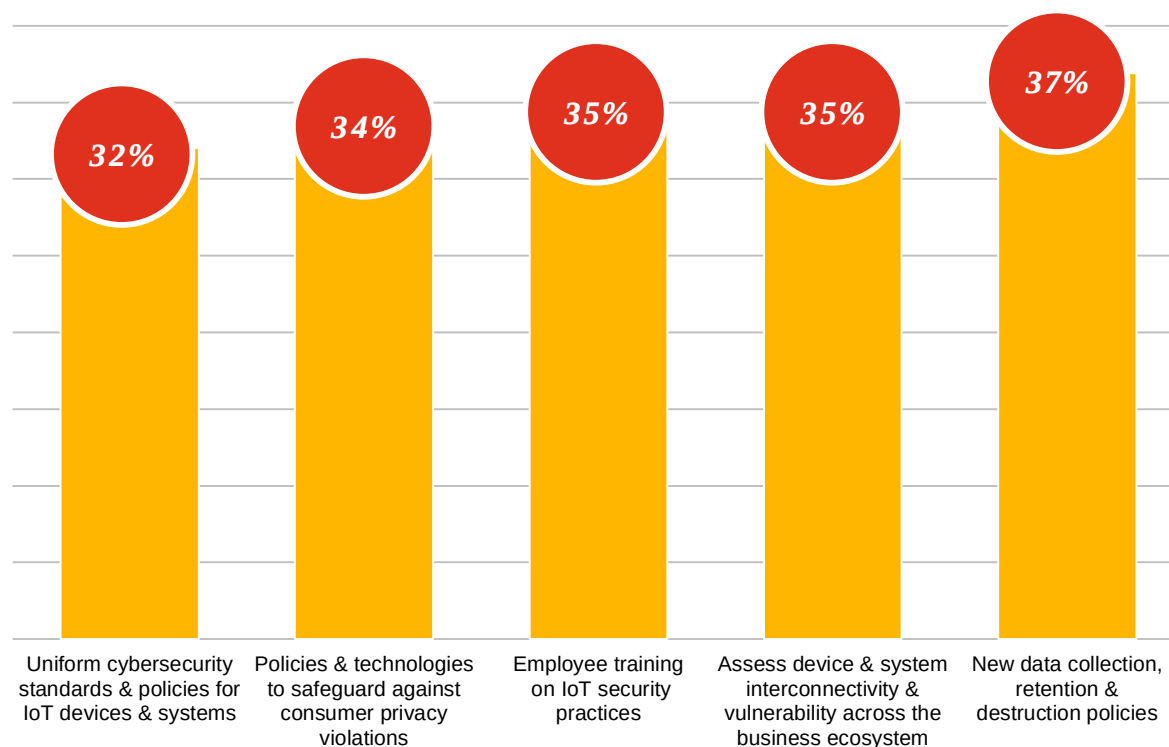
Cite phishing attacks, making it the No. 1 vector of cybersecurity incidents this year

Question 22: "How was your organization impacted by the security incidents?" Question 19: "How did the security incident(s) occur?"

As the Internet of Things takes off, organizations are moving to update their cybersecurity and privacy safeguards.

Key initiatives address data governance, device and system interconnectivity, and employee training. Consumer privacy is also a priority.

Policies, technologies & people skills being implemented for the Internet of Things



Are investing in
a security strategy
for the Internet
of Things

Question 25_2017: "What policies, technologies and people skills does your organization plan to implement over the next 12 months to address the cybersecurity and privacy risks associated with the Internet of Things (IoT)?" Question 10A_2017: "What types of security safeguards does your organization plan to invest in over the next 12 months?"

Contacts

Pavol Adamec

Director, PwC Slovakia

Tel.: +421 903 702 339

Email: pavol.adamec@sk.pwc.com

PwC firms provide industry-focused assurance, tax and advisory services to enhance value for their clients. More than 161,000 people in 154 countries in firms across the PwC network share their thinking, experience and solutions to develop fresh perspectives and practical advice. See www.pwc.com for more information.

© 2017 PricewaterhouseCoopers Slovensko. All rights reserved. In this document, “PwC” refers to PricewaterhouseCoopers Slovensko, s.r.o., which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity. “PwC” is the brand under which member firms of PricewaterhouseCoopers International Limited (PwCIL) operate and provide services. Together, these firms form the PwC network. Each firm in the network is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way.

Ďakujeme za pozornosť