EXECUTIVE SUMMARY

Infosecurity Europe Industry Survey – Report 2015

How can organisations build resilience and balance prevention and response?

INTELLIGENT SECURITY:

PROTECT. DETECT.
RESPOND. RECOVER.

Europe's most comprehensive convergence of information security professionals

infosecurity® EUROPE

SURVEY SAMPLE:

INFOSECURITY EUROPE SURVEYED 1,336 INFORMATION SECURITY PROFESSIONALS

90% MALE

10% FEMALE

Europe 78.2%
Rest of the world 16.8%
US 5%

TOP-FIVE STATUS:

10%	Board level
13%	Director level
24%	IS/IT Management
19%	Technical specialists
14%	Consultant

COMPANY BREAKDOWN:

Private sector	48%
Public sector	25%
Vendors	27%

DOWNLOAD THE FULL REPORT

EXECUTIVE SUMMARY

Information security is an industry on the rise. Major security breaches have recently been in the spotlight, and a staggering 42.8million security incidents have been reported globally (PricewaterhouseCoopers). Infosecurity Europe recently surveyed 1,336 industry professionals on the subject of 'Intelligent Security' and exposed interesting insight into protecting information assets, detecting incidents and of response and recovery.

PREVENTION IS NOT ENOUGH, INCIDENT RESPONSE IS AN INCREASING PRIORITY

It is no longer a question of debate if companies will be breached, but when. Alongside a strong prevention strategy, practitioners are now investing more in response and recovery tactics. They are recognising the need to adopt a response-focused strategy, with 69% of those who participated in the Infosecurity Europe industry survey indicating that their organisation recognises the need to invest more in incident response.

EXTERNAL ATTACKS ARE CURRENTLY THE KEY CONCERN

When asked about the greatest information risk facing their organisation today, 32% of survey respondents cited external threats such as hacking, malware, APTs / Advanced threats and DDoS attacks as their biggest concern. Recently, high-profile hacks such as Sony Pictures have highlighted the potentially devastating consequences of external attacks. Not only costly, security breaches can severely damage a firm's reputation.

Information security vulnerabilities such as Heartbleed and Shellshock, and breaches such as JPMorgan and Target have raised the profile of cyber risk, helping businesses to understand the level of risk. 67% of Infosecurity Europe industry survey participants revealed that recent high-profile breaches had a positive effect on making the business understand the potential threats.

MOST BREACHES ARE DETECTED WITHIN 7 DAYS

As the number of attacks increases, having robust and rapid detection strategies in place has never been more critical, to minimise the business impact. Although many recent breaches revealed long detection periods, the Infosecurity Europe industry survey results suggest that organisations today are discovering breaches quickly, with 62% of participants claiming to be able to detect a breach within 7 days. However, there is still a way to go for some, as 2% said that it took at least a year, with a further 15% claiming not to know.

REPUTATION, REPUTATION, REPUTATION

Financial losses caused by a hack can be devastating, such as Target losing almost £110million after being breached in 2013. The Infosecurity Europe industry survey found that the main concern for an organisation is reputational damage (62%) with only 14% stating financial loss as their prime concern. Ultimately, 90% of participants felt confident that their organisation would be capable of effectively recovering from a significant breach.

According to those who took part in the survey, the two biggest priorities facing an organisation in the wake of a security breach are minimising the impact on the customer (34%) and business continuity (31%). Organisations need to find ways of enabling business continuity and protecting their customers. According to the survey results, the most essential element of a successful incident response strategy is the ability to continually evolve the incident response plan to incorporate lessons learned.

DOWNLOAD THE FULL REPORT

INFOSECURITY EUROPE INDUSTRY SURVEY

REPORT 2015

infosecurity EUROPE

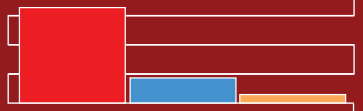
INTELLIGENT SECURITY: PROTECT. DETECT. RESPOND. RECOVER.

SURVEY SAMPLE:

INFOSECURITY EUROPE SURVEYED 1,336 INFORMATION SECURITY PROFESSIONALS

90% MALE

10% FEMALE



Europe 78.2%

Rest of the world 16.8%

US 5%

TOP-FIVE STATUS:

10%	Board level
13%	Director level
24%	IS/IT Management
19%	Technical specialists
14%	Consultant

COMPANY BREAKDOWN:

Private sector	48%
Public sector	25%
Vendors	27%

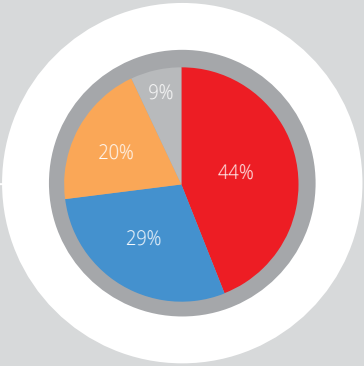
DOWNLOAD THE FULL REPORT

To what extent are your organisation's information security priorities evolving from a prevention based strategy to a response focused strategy?

- **35%** Are seeing a significant change in focus to a strategy that balances prevention and response
- **34%** Need to invest more in incident response, but evolution is beginning to establish a balance
- **31%** Continue to prioritise prevention with limited focus on incident response and recovery

Have recent information security vulnerabilities and high-profile breaches had an effect in making the business understand the potential threats?

- **22%** Yes, a very positive effect
- **45%** Yes, a somewhat positive effect
- **27%** They have made no difference
- **5%** I don't know
- **1%** No, they have been negative

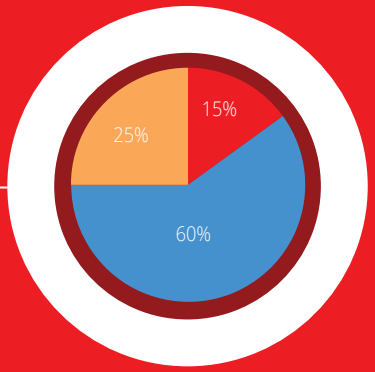


Which of the following is the biggest driver of security strategy and investment within your organisation?

- **44%** Increasingly complex threat landscape
- **29%** Meeting compliance requirements
- **20%** Fear of reputational damage following high-profile breaches and vulnerabilities
- **07%** Pressure and/or support from the board to mitigate cyber threats

In your role as an information security practitioner, which of the following has caused you the greatest concern over the last 12 months?

- **42%** Day-to-day issues (e.g. insider threat, BYOD & compliance)
- **18%** New vulnerabilities (e.g. Heartbleed and Shellshock)
- **14%** Cyber warfare and cyber espionage
- **12%** High-profile breaches (e.g. eBay, JP Morgan, Home Depot)
- **7%** Government surveillance
- **7%** Internet of Things



Has your organisation suffered a breach within the last 12 months as the result of an external attack?

- **15%** yes
- **60%** no
- **25%** don't know

Do you feel confident that your organisation understands what sensitive data the business has, and where it resides, in order to develop an effective security strategy?

- **39%** yes
- **13%** no
- **48%** somewhat

FOR MORE INFORMATION CONTACT:

Joy-Fleur Brettschneider

Joy-Fleur.Brettschneider@reedexpo.co.uk

Reed Exhibitions

infosecurity EUROPE

INFOSECURITY EUROPE INDUSTRY REPORT 2015

infosecurity EUROPE

DOWNLOAD THE FULL REPORT

What is your biggest challenge in developing a security culture within your organisation?

- **32%** Employee apathy
- **21%** Lack of buy-in, engagement and understanding from senior management and the board
- **14%** Lack of financial investment
- **13%** Ineffective security training and engagement programmes
- **9%** Lack of defined security policy
- **7%** Failure of the information security function to communicate the risks effectively, both to the board and to other stakeholders
- **4%** Failure of information security function to understand the needs of the business

Within your organisation do physical and information security functions report to the same executive business leader?

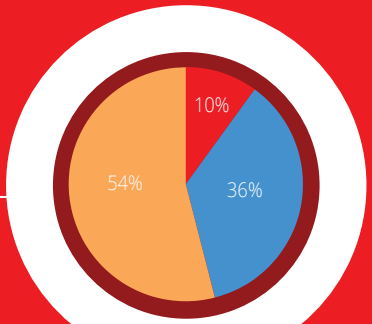
Yes 63% | No 37%

If your organisation has been breached in the last 12 months, how long after the incident was the breach detected?

28% Within 24 hours	**22%** Within 7 days	**12%** Within one hour
05% Within 28 days	**7%** Within 2 months	**06%** Within 6 months
03% Within 1 year	**02%** Over 1 year	**15%** I don't know

Within your organisation, how would you gauge your current investment in prioritising incident response in comparison with the past three years?

- **40%** We are investing more and giving it greater priority
- **39%** It has remained consistent over the last three years
- **8%** We are investing less than we have over the past three years
- **13%** My organisation does not have an information security incident response plan or capability in place



Do you feel confident that your organisation's incident response capability can effectively recover from a significant breach?

10% no | **36%** yes | **54%** limited

What do you think is the most essential element of a successful incident response strategy?

- **17%** Engaging internal and external stakeholders in incident response
- **14%** Aligning security incident response with organisational strategies
- **15%** Highly skilled incident response team with a single leader
- **17%** A clearly defined policy
- **27%** Ability to continually evolve the incident response plan to incorporate lessons learned

KEY TAKEAWAYS

1. The information security industry must **DEVELOP STRATEGIES THAT PROTECT ORGANISATIONS** whilst also building cyber resilience to ensure rapid response and recovery
2. Information security functions must **WORK CLOSER WITH BUSINESSES** - lack of buy-in from senior management was identified as a major obstacle in developing a security culture
3. **ORGANISATIONS ARE CAPABLE OF DETECTING INCIDENTS AND RESPONDING EFFECTIVELY** - only 10% claimed their organisation does not have an incident response plan or capability in place
4. **CYBER-INSURANCE ISN'T YET A KEY RISK MANAGEMENT TOOL** only 14% stated to currently be buying or considering buying cyber insurance

FOR MORE INFORMATION CONTACT:
Joy-Fleur Brettschneider
Joy-Fleur.Brettschneider@reedexpo.co.uk

infosecurity EUROPE