FUJITSU

Cyber security: predictions for 2017

Cyber Security is always presenting new challenges, and staying ahead of each year's fresh security threats is no easy task. But with a little more care and foresight, companies could have prevented many of the attacks that happened in 2016.

Will 2017 be the same?
Will companies be more pro-active about their security?
Read on to find out Fujitsu's ten cyber threat predictions.

1

Watch out for those network blind spots

Security blind spots such as PowerShell will continue to be the Achilles heel of many companies who overlook the risks they present.

2

Will smarter computers make for smarter security?

Computers are getting smarter. They're learning new tricks. And this means completely new ways of looking at security. But watch out. Hackers are using the same tricks to get past your security controls.

AI ****
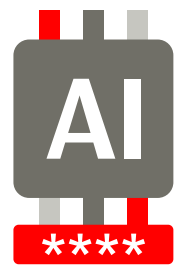
3

Banks will still be in the firing line

Last year hackers slipped through security cracks to get their hands on millions of dollars from major banks. Even with counter-measures in place, more attempted attacks on banks are likely to happen this year.
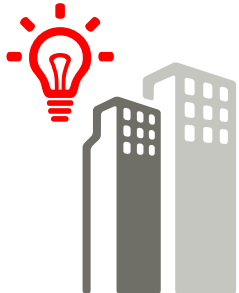
4

Attackers will shift their attention to mobile devices

You're probably looking at this on a phone right now. Is it safe? Be careful of new attacks that threaten your personal data, such as ransomware holding your photos hostage.

5

We'll see how clever "smart cities" really are

The designer of smart motorway noticeboards probably didn't think that someone would hack them to display political messages. Smart systems will be tested to their limit. Keep an eye on your control platforms.
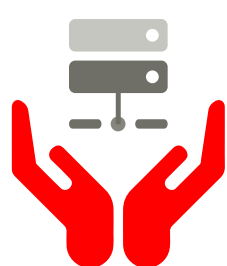
6

Rapid recovery required, to protect reputations

No matter what security controls you have in place, companies are going to get hacked. If you don't recover quickly, it will hurt your business and reputation. Are you ready for the challenge?
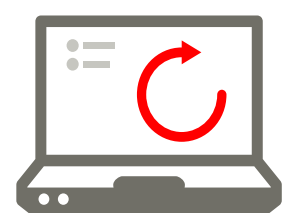
7

Businesses will want their data in the safest hands

The General Data Protection Regulation is just around the corner. That means investors, shareholders, customers and regulators will want their data kept as safe as houses.

8

Global clients will keep a beady eye on supply chains

You might have secured your sensitive data, but has your supply chain? Big businesses will only want to work with supply chains that know how to handle data security.
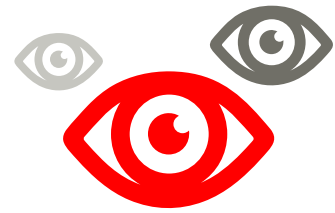
9

Boards will want to talk IT security

Boards are waking up to the truth. Bad IT security is bad for business, both in terms of revenue and branding. But they can't always get their heads around the technical jargon, so senior IT staff will need to discuss their needs in a language they understand.

10

The biggest problem will still be the basics

We would like to say that all your security ills will be down to sneaky cyber hackers. The real villain is much more boring. Failure to keep up with basic IT practices will be what leaves you open to breaches.
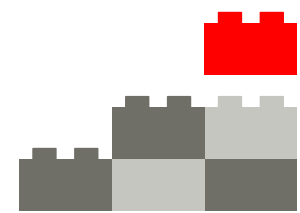
If 2016 has taught us anything, it's that companies ignore developments in cyber security at their own risk. Although no-one is invulnerable to attacks, if you stay organised and vigilant, you'll stand a much better chance of avoiding them and the business disruption they can cause.

Visit the Secure Thinking website to find out more about keeping your business protected from cyber threats.

FUJITSU