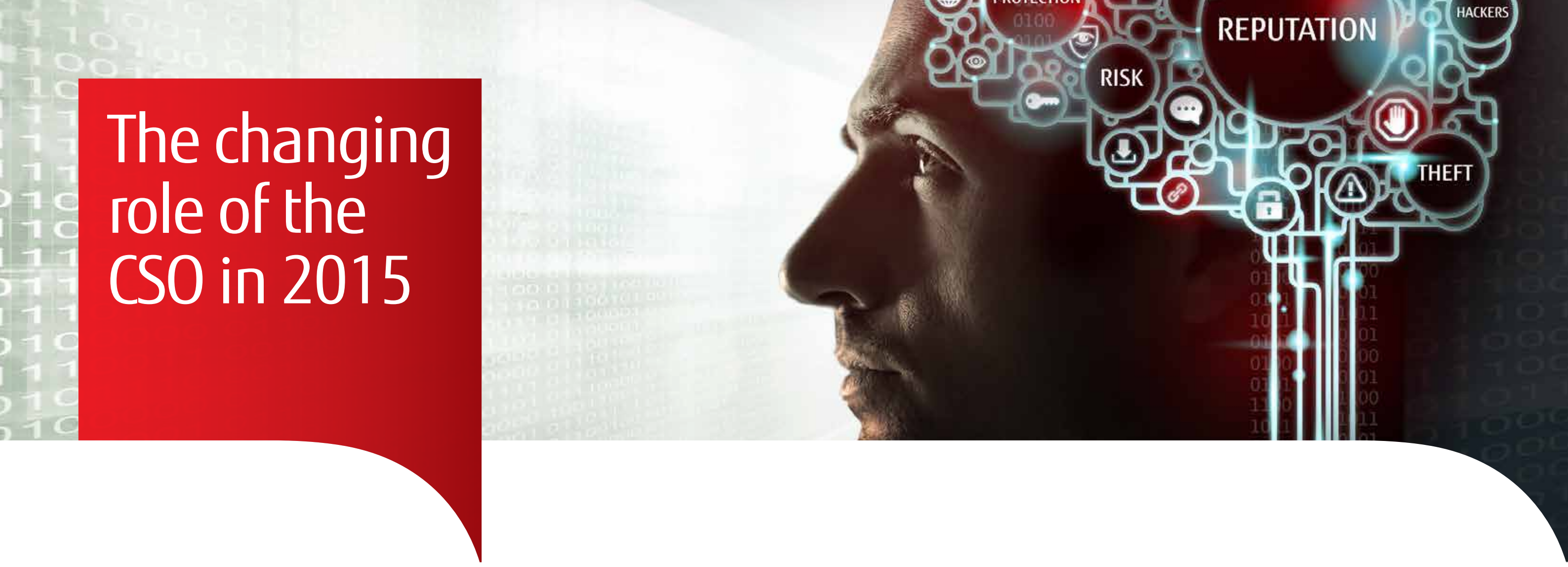
The changing role of the CSO in 2015



The year in review following the Check Point Security Report 2014

Fujitsu specialist ICT security partner Check Point produces an in-depth report into the evolving cyber threat landscape every year. After high-profile data breaches, information security rose to new levels of prominence in the public consciousness in 2013. Covered in its 2014 report, Check Point identified the emerging trends and their potential impact on Chief Security Officers (CSOs).

In a new prologue to the full report, our security expert Rob Lay, examines those predictions from 2014 and outlines the changes CSOs should prepare for as we move into 2015.

The explosion of unknown malware

The 2014 Check Point report stated that attacks via unknown malware were expected to increase. While these would require additional security measures, updating traditional security technologies such as anti-virus and intrusion prevention systems could make life harder for hackers who will always test new malware against existing security systems.

Rob's view:

» We have certainly seen an increase in the volume of malware. What it means is that businesses have to focus on making sure that basic security platforms or technologies are working properly. This takes away some of the 'attack surface' from the attackers. Attackers are always going to be lazy and use the easiest way to get into the business. Without anti-virus and other protection in place then it makes life much easier for the attackers.

Two or three years ago, organisations were much more complacent. However, the threat landscape continues to evolve. The significant volume of infected files, such as PDFs, brings security training and awareness back into play for CSOs. A lot of the ways hackers get this unknown malware into organisations is through human beings clicking on infected files and dodgy emails or links. CSOs have to drive security awareness training and the change in organisational culture because this sort of thing always requires leadership.«

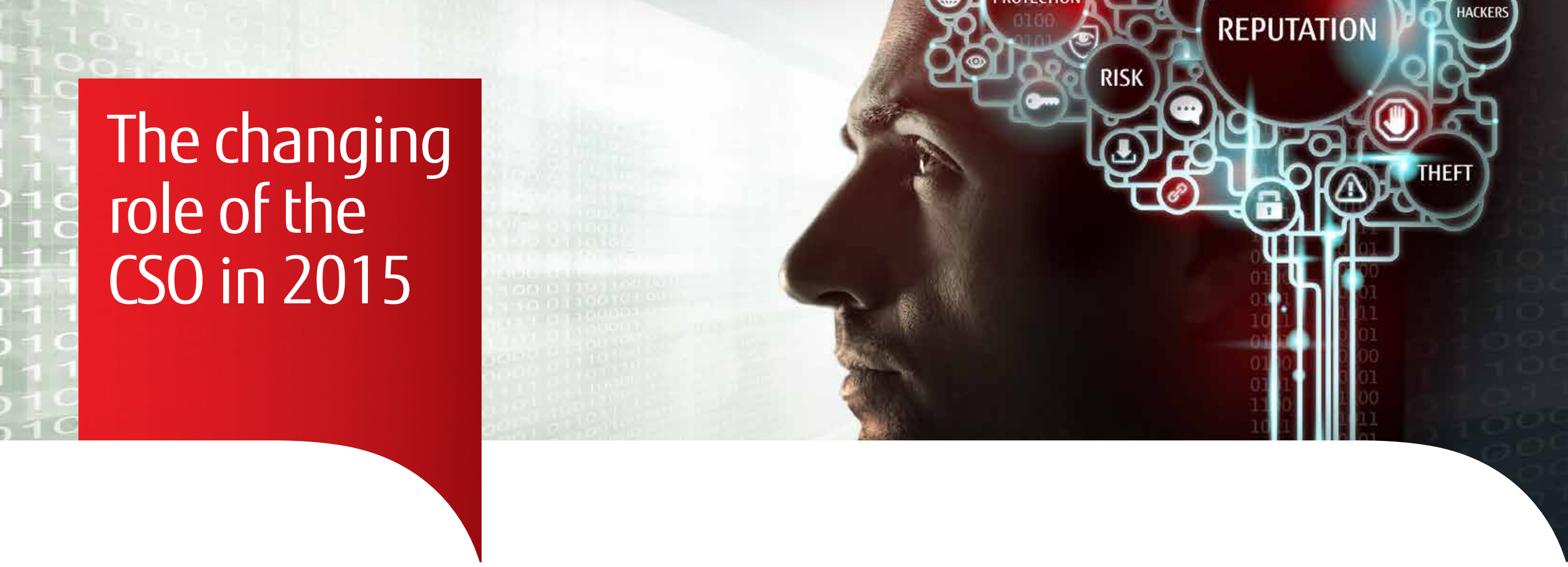
Need to know:

35%

of files infected with unknown malware are PDFs

shaping tomorrow with you

The changing role of the CSO in 2015



The devil you know

The rise of malware is not just about targeted attacks. Success in recent years has come from employees clicking on links or sharing infected files. In 2012, less than half (43%) of organisations analysed by Check Point experienced a user downloading malware at a rate of less than one per day. In 2013, almost two-thirds (58%) experienced users downloading malware every two hours or less.

» For the organisations I am working with in the UK, malware is a constant threat. Trying to maintain signature updates and anti-virus protection is a constant challenge – particularly with a very mobile workforce using laptops, tablets and smartphones.

This is an operational challenge for CSOs. It is about protecting the business from day-to-day threats rather than a strategic issue. Looking ahead, CSOs need to ensure the business is able to respond faster to new threats. They can do this by understanding which areas of the business are most important and need protecting and then focusing resources and training there.«

Need to know:

10 mins

the frequency with which a host downloads malware

App(etite) for destruction

Applications are essential to productivity but they also create degrees of vulnerability in any company's ICT security. Check Point noted the rise in high-risk applications enabling anonymous web surfing, cloud-based storage and sharing of files as well as the remote use of desktops. Whether officially sanctioned, part of a creeping 'shadow IT' or unknown to IT teams, there is a growing number of applications operating within corporate networks with little or no oversight.

» This is a very real risk for CSOs. Most are aware of it; some are struggling with it. But it comes back to a fundamental point about security. For a long time, security has been seen as something that stops the business from working. But security has to be an enabler. One CSO I spoke to recently decided that instead of saying 'No, you can't do that' he would pre-vet applications and cloud platforms that the business could use. Then he could say, 'Go and use these ones', while knowing they would pose little risk to the business while helping his colleagues.

When it comes to social media, these are now fully entwined with the business. There is no getting away from that and CSOs also need to educate colleagues so that when they use social media they are aware of the security issues. CSOs now need to find a way for colleagues to embrace these new technologies without bringing too much risk into the business. As Gartner identifies, it's about understanding your risk profile and how to manage it.«

Need to know:

85%

of organisations were found to be running Dropbox on their systems

The changing role of the CSO in 2015

Need to know:

88%

of organisations experienced at least one data loss incident in 2013

Data loss incidents

Major attacks involving millions of consumers have brought data loss incidents to the fore. But now there are more ways than ever for data to fall into the wrong hands. Mobile devices, shadow IT and the Internet of Things exacerbate the situation as more data is shared in more ways. And it is not just large organisations that are at risk. In 2013, Check Point cites a range of examples of data losses that had nothing to do with hackers and provides evidence that these forms of breaches are on the rise.

» A lot of the focus on malware in recent years has been on how people get into the organisation. CSOs also need to focus their attention on how people can get data out. This covers more than hacking but also breaches that begin internally – such as theft or accidental loss.

A CSO's Data Loss Prevention (DLP) solution needs to cover more than cyber attacks. It needs to identify where things can go wrong within the organisation and help put a stop to it. Rather than waiting for something to happen, putting in place the people, processes and technologies to be more proactive can prevent or minimise the impact of significant losses.«

Need to know:

144%

increase in new malware found from 2012 to 2013

The security architecture for tomorrow's threats

The findings within the 2014 Check Point report indicate that while the threat landscape continues to evolve many security strategies have not. There is wide proliferation of point security products but today's corporations need a single architecture that combines high performance network security devices with real-time proactive protections. Check Point calls this Software Defined Protection.

» Businesses have recognised that the threat landscape has changed. Businesses are having to be more agile and do things quicker to remain competitive in their markets. On top of that, pretty much everything they do these days is digital in one form or another. The only way to deal with all of this is to create some sort of framework or architectural approach to security.

This will allow CSOs to implement security on a consistent basis so they can be flexible and fast in responding to changing threats. The first step on this journey for CSOs in 2015 is to understand more about where they are already and where they need to be. Secondly, it is about adding context to security. What is the threat and how does it affect my business? Armed with that information, CSOs can take decisions on how to respond with security resources or go to the board for investment based on real business outcomes.«

View the Check Point 2014 report

For more information, please visit:

uk.fujitsu.com/securethinking

#securethinking

shaping tomorrow with you

Check Point
SOFTWARE TECHNOLOGIES LTD.

FUJITSU