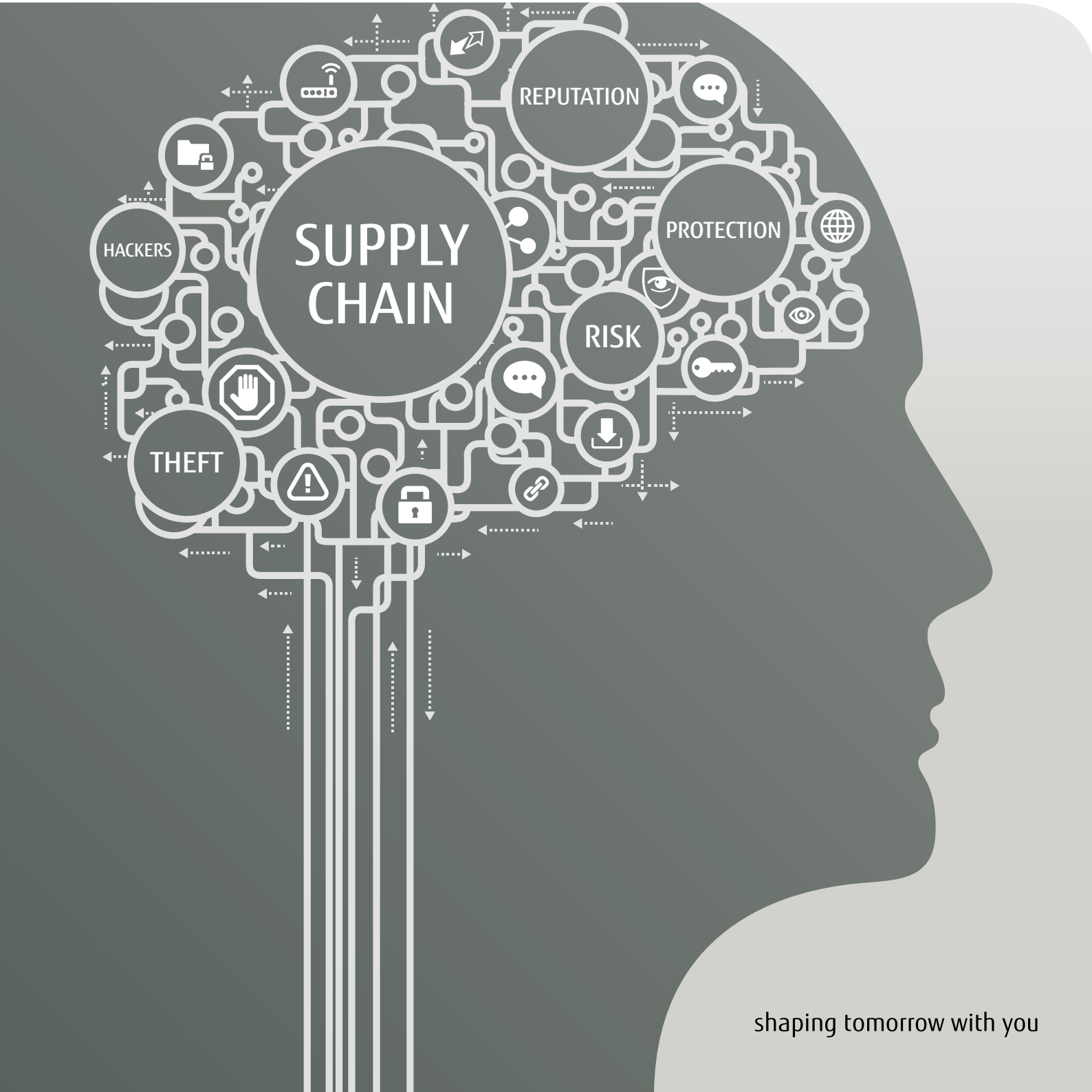
FUJITSU

Securing the supply chain:
What every organisation needs to know



shaping tomorrow with you

Security breaches are becoming more commonplace as hackers, cyber criminals and terrorists use ever more sophisticated attacks. In 2013, 93% of large organisations and 87% of small businesses experienced a security breach. Those public and private sector organisations affected experienced around 50% more breaches on average than the year before.[1]

In an increasingly distributed world, meanwhile, organisations continue to outsource activity for good financial reasons. According to the Economist, for example, many of today's manufacturing firms outsource between 70-80% of the content of their finished products to suppliers.[2]

Consumers are also much closer to suppliers than ever before, so that their personal data is now often shared directly with third parties. To take just one example, in retail, customers regularly provide key details to delivery partners without the retailer being involved in the process.

Such developments have led to a new source of IT security risk: **the supply chain.**

Suppliers are now one of the most vulnerable areas in any organisation's security strategy. Larger or better-protected organisations are not worth the effort for hackers – especially when there are easier ways to steal, manipulate or damage mission-critical data further down the supply chain.

But before tackling the issue of IT security across a supply chain there are key elements every organisation should take into consideration.

[1] https://www.gov.uk/government/publications/information-security-breaches-survey-2013-technical-report
[2] www.economist.com/media/globalexecutive/outsourcing_revolution_e_02.pdf

Analyse the supply chain.

Fujitsu in the UK and Ireland has [xxxxxx] suppliers while support services provider Carillion has 20,000[3] and supermarket giant Tesco has 2,000 own-brand primary suppliers alone[4]. These primary suppliers will have their own primary and secondary suppliers too.

If asked, could you identify your key suppliers? Furthermore, which companies then supply your main suppliers?

By mapping your entire supply chain and the links to competitor organisations you will start to build up a picture of where the biggest IT security threats to your business reside. This information is critical in developing a robust plan for securing the entire supply chain.

Such a plan of action is a big task and likely to require significant time and effort before it is fully achieved. As a result, it is helpful to know where the major weaknesses are and address these first. The best place to start is by identifying the business impact of a particular security threat and then prioritising action accordingly.

Understand the risk

As the Government's Security Breaches Survey for 2013 showed, the financial impact of a security breach can be extensive. The worst security breaches alone cost large companies on average £650-850,000 and small companies £35-65,000.[5]

How you control your suppliers is a big problem in terms of reputational risk too. Bodies such as the European Commission and Financial Conduct Authority are now taking steps to ensure CEOs hold more responsibility for their suppliers and trading partners to provide greater risk assurance. The Information Commissioner's Office even has the power to fine organisations up to £500,000 for failing to prevent data breaches.

Worryingly, with such huge financial and reputational risks, the Government's survey showed that nearly a quarter (23%) of all organisations had not carried out any form of risk assessment.

Only a thorough audit can show you which points in your supply chain are vulnerable.

[3] http://blog.supplymanagement.com/2010/11/how-many-suppliers-is-the-right-number/
[4] www.tesco.com/csr/downloads/pdf4.pdf
[5] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/191671/bis-13-p184es-2013-information-security-breaches-survey-executive-summary.pdf

Find the weakest link(s).

Following the flow of mission-critical data through your supply chain will help you identify specific weaknesses. In the eyes of regulators and consumers alike, the responsibility for this data lies squarely with your organisation so it certainly pays to know where it ends up.

This involves working directly with core partners as well as those less obvious but equally important players in your supply chain – international distributors or overseas component manufacturers for example.

After having mapped your suppliers you will need to ask what they do with your data. What information goes where and how is it passed on to third parties? Who do they pass it on to in turn?

Key questions for interrogating your supply chain:

- Who are your suppliers?
- Who are their suppliers?
- How do you exchange data?
- Do you understand who does what with your data?
- Do they really need it?
- What is the business risk of losing this data?
- What regulations govern the flow of your data at home and abroad?

Introduce a security standard

Traditionally, the most common way to create supplier risk profiles was to email a simple self-assessment spreadsheet questionnaire.

These may have included questions relating to international standards, such as ISO27001, as well as internal requirements but there would be no standard template for the entire supply chain.

With primary suppliers then expected to profile their suppliers in turn the administrative process would see hundreds, if not thousands, of spreadsheets in circulation between multiple stakeholders.

This lack of centralised management led forward-thinking organisations to shift supply chain audits from self-assessment spreadsheets to independent audit.

Despite outsourcing the audit process, these companies are regaining control over supply chain security. They now benefit from full visibility of supplier risk as well as the economies of scale that come with a standardised process. Furthermore, they ensure compliance with the latest industry best practice - for example, Chapter 15 of the new ISO27001 standard covering supply chain management.

Take action.

A full supply chain security audit is a considerable task, especially when you have several hundred suppliers or more. To improve your supply chain security you first need to know who your suppliers are and categorise them based on a standardised risk assessment.

Whether you choose to profile your supply chain internally or ask for an independent audit, technology, such as the **Symantec Control Compliance Suite**, can reduce the associated time, effort and costs.

Once the audit process is complete then securing your supply chain IT security becomes an easier process. Armed with risk profile information that you can rely on, you can create robust Service Level Agreements that have specific IT safeguards built in. Only when these are in place can you be sure that your organisation is protected from security threats and the negative financial or reputational impact that inevitably follows.

Concerned about your supply chain security?

Download the datasheet to learn more about what you can do to protect your organisation. >>


Data Sheet Supply Chain

FUJITSU

Fujitsu Security - Supply Chain

Do you know how many companies are in your supply chain?
How serious would it be if any supplier lost your mission-critical data?
What action can you take to mitigate such risks?

SUPPLY CHAIN

Step 1 – Audit

Symantec Control Compliance Suite - Vendor Risk Manager

Key benefits