Weak links

Strengthening the information supply chain

July 2015

Information supply chains are becoming more complex as organisations make increasing use of online interaction to support business processes. This involves all organisations, not just those with physical supply chains. The choice is not whether to share data with others, but how securely this is done.

Priorities vary depending on the types of data being shared and this includes the choices made in the supporting security capabilities. Those that place the highest value on payment card data, personal data, intellectual property and software code all invest more than average in various security capabilities as do those with the most complex information supply chains.

Bob Tarzey
Quocirca Ltd
Tel : +44 7900 275517
Email: Bob.Tarzey@Quocirca.com

Rob Bamforth
Quocirca Ltd
Tel: +44 7802 175796
Email: Rob.Bamforth@Quocirca.com
Executive Summary

Weak links

Strengthening the information supply chain

All organisations now have to manage an online information supply chain, this is a given. What varies is the complexity and types of data involved. The security choices being made by those already pushing the information supply chain to its limits are a guide to those that will inevitably follow in their steps.

All organisations have to manage an information supply chain

Regardless of whether there is an underlying physical supply chain, all organisations now have to manage an online information supply chain. The range of organisations involved in the chain is broad including business customers, partners, suppliers, contractors, consumers and regulators. The requirement to share data externally is a given for 21st Century businesses; the only choice is how safely this is done.

Information supply chains are becoming more complex

As more and more parties get drawn in, the information supply chain becomes increasingly complex. This is also impacted by globalisation. Those UK-based organisations that trade across the EU or around the globe have more complex information supply chains. Manufacturers have more complexity, due to the number of intermediaries involved in their physical supply chains and their global reach. Financial services organisations have the least complexity.

Complexity is supported by advanced security

The more complex an organisation’s information supply chain is the more it is likely to invest in information security. This includes improving user knowledge about security and better coordination of security policy and incident response along with the use of more advanced security capabilities.

Certain data types cause more concern than others

Of greatest concern is payment card data, followed by personally identifiable data and intellectual property (including software code). Emails, word processor files and spreadsheets are lower on the list, not because they are considered unimportant, but because focussing in on more specific types of data protects the information embedded in such documents anyway.

The data types of most concern vary by industry sector

With tighter regulations in Europe, personally identifiable data is high on the list of concerns for most organisations. Payment card data worries retail, distribution and transport organisations above all else. Manufacturers worry most about the intellectual property and software.

Investments vary depending on the data types involved

Although it is the data type of most concern, payment card data is least likely to motivate increased investment; this is because the problem can be largely outsourced via payment gateways. This is not the case with other data types where certain specific protections are sought, especially to help enable safe sharing of data in the cloud and protect what happens to data on user end-points.

High complexity also drives security choices

Those with the highest levels of supply chain complexity are more likely than average to have deployed capabilities for controlling user end-points and user behaviour. This reflects the fact that they are often manufacturers or commercial organisations, where end-points are in use on shop floors and in the field. Such organisations are also less likely to be tolerant of bring-your-own-device.

Conclusions

As online information supply chains become more complex organisations are investing more in IT security to protect the data that underpins them or is made vulnerable by their openness. A haphazard approach to security is unlikely to work; organisations that value, or worry about, certain types of data are using specific security capabilities to provide focussed protection.
Introduction - the information supply chain

Physical supply chains are now usually managed through online interaction, this leads to a second supply chain over-laying the first – the information supply chain. However, this information supply chain is not limited to those organisations that deal with the movement of physical goods, far from it; it has become fundamental to the activity of most business, from old world banks and law firms to the new world social media providers.

The parties involved in the information supply chain range from suppliers, through consumers, business customers, partners, contractors to regulators (Figure 1). Examples include online retailers sending goods to consumers via delivery firms after confirming transactions via payment gateway providers; wholesale suppliers who receive orders from outlets online and then ship via distributors whose agents confirm delivery via mobile phones; law firms sharing case documents electronically with the other firms and the courts and any firm providing accounting information to its auditors.

The advent of the information supply chain has provided many benefits, for example improved automation, as discussed in a 2013 Quocirca report, Customer automation management. However, it also introduces new risk. By definition information supply chains involve many organisations and any one of these can be a weak link. The pressure to protect data can come as much from supply chain partners as it does from regulators.

The benefits of well-connected information supply chains can only be realised if appropriate security is in place and this extends to all the parties involved. The choice is not whether to share data with others, but how it is done.

Information supply chain complexity

A particular organisation can be given a crude score for its information supply chain complexity depending on the number of different types of entities that it transacts with online. For the analysis presented in this report, based on data shown in Figure 1, the minimum score is 1 (as no respondent said its organisation dealt with no outsiders at all) and the maximum is 6. This score can then be used to measure average supply chain complexity, for example by sector (Figure 2).

Manufacturers, by their very nature, have complex physical supply chains involved with the movement of parts and products that lead to more complex information supply chains. Financial services firms have the least complexity on average; this is down to fewer intermediaries being needed for the electronic movement of funds, but also because some more conservative organisations, such as insurance companies have been slower to bring certain processes fully online.
Information Supply chain complexity is also impacted by globalisation. More than half of UK organisations with more than 1,000 employees now trade internationally, especially manufacturers and commercial organisations. There is little difference between businesses of different sizes (Figure 3). Globalisation leads to more complex information supply chains (Figure 4).

Overall, regardless of sector, organisations that are advanced in exploiting connectivity will also have more complex information supply chains as they engage online with a broader range of customers, partners and suppliers. Given the general drive for increasing numbers of business processes to be managed online, information supply chains can only be expected to become more complex. In other words, those with a lower information supply chain complexity score today can expect it to increase in the future. They can learn from what the vanguard are already doing to put in place supportive security.
Data that matters

A previous Quocirca report, based on the same research – *Room for improvement: Building confidence in data security* – looked at the drivers behind confidence in data security. These included better employee knowledge, the use of advanced security technology and co-ordinated security policy and incident response. The degree to which organisations embraced these three areas was used to derive a composite security score that ranged from very low to very high. There is a strong relationship between information supply chain complexity and the composite security score indicating a willingness or necessity to invest in security as the information supply chain complexity increases (Figure 5).

Of course, there is an element of chicken-and-egg to this, do complex information supply chains motivate security investment, or does security investment come first, to enable more complex information supply chains? Either way, those with more complex information supply chains are more likely to be investing more in security capabilities.

Some data types are of greater concern than others when it comes to security (Figure 6). Overall, payment card and personal data top the list. These are highly regulated data types, but that is for a reason, they are also the ones of most value to criminals. The concern businesses have about such data is to do with more than just being compliant – it is a recognised need to protect relationships with customers, partners, suppliers and consumers and to protect overall reputation.

Email, spreadsheets and general word processor documents are the least likely to be considered very important. This is because data, is not the documents themselves but their content. So, if effective security, such as data loss prevention (DLP) is in place to protect the movement of payment card data and intellectual property, then this covers all these document types anyway. In other words, the more focussed that data protection is, the better.

---

**Figure 5: Supply chain complexity motivates security investment**

<table>
<thead>
<tr>
<th>Composite security score</th>
<th>Average information supply chain complexity score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very high</td>
<td>4.44</td>
</tr>
<tr>
<td>High</td>
<td>4.07</td>
</tr>
<tr>
<td>Medium</td>
<td>3.64</td>
</tr>
<tr>
<td>Low</td>
<td>3.39</td>
</tr>
<tr>
<td>Very low</td>
<td>2.80</td>
</tr>
</tbody>
</table>

**Figure 6: Importance of security concerns with regard to various data types**

<table>
<thead>
<tr>
<th>Data type</th>
<th>Very important</th>
<th>Fairly important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment card data</td>
<td>61%</td>
<td>20%</td>
</tr>
<tr>
<td>PID</td>
<td>57%</td>
<td>37%</td>
</tr>
<tr>
<td>Blueprints</td>
<td>51%</td>
<td>33%</td>
</tr>
<tr>
<td>Software code</td>
<td>45%</td>
<td>36%</td>
</tr>
<tr>
<td>Email</td>
<td>37%</td>
<td>54%</td>
</tr>
<tr>
<td>Spreadsheet</td>
<td>37%</td>
<td>51%</td>
</tr>
<tr>
<td>WP Docs</td>
<td>20%</td>
<td>49%</td>
</tr>
</tbody>
</table>

**Full description of data types as used in survey**

- Payment card data
- PID – Personally identifiable data
- Blueprints – blueprints, design documents
- Software code – software source code
- Email
- Spreadsheets
- WP Docs - general word processor documents
Unsurprisingly concern varies by industry (Figures 7-10). For retail, distribution and transport, payment card data is by a long measure the greatest concern. Financial services worry about payment card data too, but personal data is of equal concern. For manufacturers intellectual property tops the list as concerns about both cyber-espionage increase and the insider threat increases.
The composite security index shows that, for the four data types of greatest concern in the information supply chain; payment card data, personally identifiable data (PID), intellectual property (IP) and software code; considering any one of them very important leads to more security investment (Figure 11). Payment card data is an exception, in that just considering it fairly important also leads to higher levels of investment.

The index itself was derived from responses to the following three questions, which provide the detail about where this investment is being channelled:

Which of the following data and/or user protection measures do you have in place?
7 options given – blue in Figures 12-16

Which of the following measures do you have in place to make sharing data in the cloud more secure?
5 options given – red in Figures 12-16

Which of the following user end-point security and/or management capabilities do you have in place?
8 options given – green in Figures 12-16

Figure 12 shows deployment levels for all 20 security capabilities investigated. However, this list should not be taken at face value. Some of these least-used capabilities overall, are more likely to be used by those organisations considering a certain type of data very important, to seek to maximise protection in their information supply chain.

On average an organisation that considers any given data type very important is more likely to have invested in almost any of these security capabilities. However, it should be pointed out that many have still to do so. For example, overall 53% have invested in DLP. This rises to 60% for those that consider PID very important, meaning 40% have not.
Weak links

Payment card data
Payment card data is the primary target for many cybercriminals. It can be sold or used to pay for goods which themselves can be sold. It is in the interests of businesses that take online payments to protect their customers’ payment card details in order to maintain on-going confidence and their own reputations. Should they be in any doubt of the need to do this, the Payment Card Industry Data Security Standard (PCI/DSS) is there to remind them.

The easiest way to comply with the standard and protect payment card data is to outsource the taking of payments to a payment gateway provider such as Cardstream, CyberSource, DataCash, NetPay or WorldPay. However, even if this has been done it is still possible for an organisation to fall foul of the rules. For example, if a customer emails an order with payment card details embedded, simply through hitting reply to say thank you, the details are sent back out in the open, causing a breach of PCI/DSS. Therefore, in the sectors where it matters most, protection should still be in place to police content for payment card details, regardless of how payments are actually processed.

Those considering payment card data very important (Figure 13) are more likely to have next generation firewalls in place, which provide application level controls at the perimeter, a requirement of PCI/DSS. They are also more likely than average to put controls around what users can do on end-points with policy based access rights (for example based on device type and/or location). The end-points themselves should be more tightly controlled with configuration change monitoring and mobile app management more likely to be in place.

However, it should be pointed out that, whilst payment card data is the data type of greatest overall concern, it is the one for which an increased level of investment in various technologies is the least likely (range 8% to 13% for the top 10 compared to 9% to 23% for other data types). This is because the problem can be completely outsourced, which is not possible for other high priority data types.

Personally identifiable data (PID)
Stolen personal data has a number of uses. In many cases, it is used to phish for more information and to get users to give away access credentials, allowing hackers to gain entry to systems for whatever reason. In some circumstances it may be used to embarrass or bribe. In the EU personally identifiable data is tightly controlled and will become more so with the new General Data Protection Regulation set to become law later in 2015 or 2016. To this end, the need to protect PID is driven by regulatory fear to a greater degree than is so for other data types.

Personally identifiable data is too broad a category to outsource responsibility for, as can be done with taking payments. The protections in place need to be pervasive, including monitoring for certain give-away data types, such as: National Insurance Numbers, birth dates, passport details and of course, payment card details. Figure 14 shows that those considering personal data very important are more likely to have above average investment in policy based access rights, user end-point configuration controls and mobile application management. The top ten includes 4/5 of the cloud data sharing capabilities investigated.
Intellectual property

There is no pervasive regulation of intellectual property. However, there are circumstances where auditors and industry bodies would become concerned if intellectual property was known to be compromised, for example during merger talks and when valuing a company’s assets. The need to protect intellectual property is more value-driven, much of which is lost if it gets into the hands of competitors by direct theft or being sold on by an intermediary. Hacktivists may steal and publish intellectual property just to spite an organisation they dislike.

The motivation to steal intellectual property should not be under-estimated. It is not beyond employees of one UK-based company to steal from another, even if not sanctioned by management, especially when they are on the move to another employer. The insider threat is considered to be at its greatest when an employee is thinking of moving; in fact monitoring an employee’s behaviour and the information they are accessing can be a sign that they are about to jump ship. However, the greatest threat to UK companies, especially manufacturers, is industrial espionage perpetrated by competitors and governments. Verizon’s 2014 Data Breach Investigation Report suggests state-affiliated actors in eastern Asia are the worst offenders.

Those considering intellectual property very important are particularly likely to have above average investment in user end-point configuration controls, policy based access rights and user behaviour monitoring (what are those insiders up to?) DLP and DRM are both in the top ten, as those organisations that value intellectual property the most, seek to control and protect it (Figure 15).

Software code
Software code is a special form intellectual property. Whereas IP, in the form of blueprints and design documents tends to be the realm of manufacturers, all organisations will have some software at their heart that drives their business and makes them competitive. Insurers have algorithms to try and ensure their quotes are slightly better than others on price comparison sites. Retailers will have software to process their loyalty schemes and keep ahead of the competition. For some business, such as software application suppliers and gaming companies, software is everything.

One of the conundrums about software is that developing it is a collaborative process, often involving third parties. The process itself benefits from the use of specialist collaboration tools for versioning and change control – this is software configuration management.

However, more general security capabilities are valued too, especially anything that helps show what users are up to on their end-points (Figure 16). Interestingly, those that value software code the most are the most likely to have above average investment in vulnerability management, perhaps being all too aware that much software is riddled with flaws.
Information supply chain complexity

As has been seen from the composite security index, information supply chain complexity itself is also a driver for increased security investment. The detail here is interesting. Figure 17 shows the top 10 above average deployments for those with a high information supply chain complexity. It includes 6/8 of the end-point security and management technologies investigated and 4/7 general user/data protection measures but none of the 5 cloud sharing measures.

Perhaps those with the most complex information supply chains, often being manufacturers and commercial organisations, are locking down company-issued end points in use in the field and on shop floors. Such organisations are also likely to be less tolerant of bring-your-own-device and in a better position to control managed user end-points. This fits with the top 3 capabilities being, activity logging on end-points, application white/black listing and user behaviour monitoring in general.

Conclusions

All organisations have to manage an information supply chain; what varies is the complexity of the chain and the data types that are involved. Both of these factors influence the decisions made about the data security capabilities that are put in place.

Overall, payment card data is of greatest concern, however, this is the least likely to drive above average security investment as those, such as retailers (that worry most) can outsource the problem to payment gateway providers. Personally identifiable data is high on the list of concerns of most organisations, driven by UK and EU data protection law and the threat that data leaks pose to customer confidence and reputation; this leads organisation to focus in on access rights and end-point controls. Those that worry about intellectual property also worry about access rights and end-point controls, but are also more likely to have invested in DLP, DRM and user activity logging.

The more complex an information supply chain is, the more likely an organisation is to lock down user end-points that are in use in the field or on shop floors; this being seen as more effective than broader controls around access to cloud based resources. Typically these are manufacturers and commercial organisations.

A haphazard approach to data security will not be effective. Organisations that value, or worry about, certain types of data the most are using specific security capabilities to provide focussed protection. Those that are yet to apply such focus can learn from the security investment decisions that the vanguard have already made.

References

1 – Quocirca, October 2013, Customer automation management, Dealing with diversity: there is more to serving customers than EDI http://quocirca.com/content/customer-automation-management
2 – Room for improvement: Building confidence in data security – available free from Quocirca on request
Appendix 1 – Demographics

All respondents were from UK-based businesses. The industry sectors, business sizes and job roles are shown below:

**Figure 18: Industry sectors by size**

<table>
<thead>
<tr>
<th>Industry Sector</th>
<th>&gt; 3,000 employees</th>
<th>1,000 to 3,000 employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>R&amp;D</td>
<td>13</td>
<td>12</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>13</td>
<td>12</td>
</tr>
<tr>
<td>Other commercial</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>Financial services</td>
<td>12</td>
<td>13</td>
</tr>
</tbody>
</table>

**Figure 19: Job roles (actual sample numbers)**

- CEO: 41
- CIO/IT Director: 21
- IT manager: 2
- App mgmt/bz analyst: 4
- Infosec manager: 32

**About Digital Guardian**

Digital Guardian offers security’s most technologically advanced endpoint agent. Only Digital Guardian ends data theft by protecting sensitive data from skilled insiders and persistent outside attackers. For over 10 years we’ve enabled data-rich organizations to protect their most valuable assets at the endpoint. Our unique contextual awareness, transformative endpoint visibility, and flexible controls let you minimize the risk of data loss without slowing the pace of business.
About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first-hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation’s environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to provide advice on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca’s mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca’s clients include Oracle, IBM, CA, O2, T-Mobile, HP, Xerox, Ricoh and Symantec, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca’s work and the services it offers can be found at http://www.quocirca.com

Disclaimer:

This report has been written independently by Quocirca Ltd. During the preparation of this report, Quocirca may have used a number of sources for the information and views provided. Although Quocirca has attempted wherever possible to validate the information received from each vendor, Quocirca cannot be held responsible for any errors in information received in this manner.

Although Quocirca has taken what steps it can to ensure that the information provided in this report is true and reflects real market conditions, Quocirca cannot take any responsibility for the ultimate reliability of the details presented. Therefore, Quocirca expressly disclaims all warranties and claims as to the validity of the data presented here, including any and all consequential losses incurred by any organisation or individual taking any action based on such data and advice.

All brand and product names are recognised and acknowledged as trademarks or service marks of their respective holders.