Cyber security: A critical examination of information sharing versus data sensitivity issues for organisations at risk of cyber attack

Jason Mallinder and Peter Drabwell

Received (in revised form): 15th July 2013

Credit Suisse, Zürich, Switzerland
E-mail: jason.mallinder@credit-suisse.com

Jason Mallinder *joined Credit Suisse in 1998, initially managing the Access Control team in London. During his time at the bank, he has managed a number of teams and programmes in the identity management and IT risk management areas. In July 2011, Jason moved to focus on operational risk management within the investment bank for a year, before returning to technology risk management as the EMEA regional head. Prior to joining Credit Suisse, Jason worked at Aon Risk Services for seven years and he has supported his career by achieving qualifications in both risk management and project management.*

Peter Drabwell *is a senior technology risk analyst at Credit Suisse within the Risk Management division, responsible for private banking, wealth management and shared services IT clients across EMEA. Prior to joining Credit Suisse, Peter was responsible for the risk assessment of ABN AMRO/RBS IT integration, and the development of risk management strategy for mergers, acquisition and divestitures. Peter is an active member of the ISC(2) European Advisory Board and is currently President of the ISACA London Chapter.*

ABSTRACT

Cyber threats are growing and evolving at an unprecedented rate. Consequently, it is becoming vitally important that organisations share information internally and externally before, during and after incidents they encounter so that lessons can be learned, good practice identified and new cyber resilience capabilities developed. Many organisations are reluctant to share such information for fear of divulging sensitive information or because it may be vague or incomplete. This provides organisations with a complex dilemma: how to share information as openly as possibly about cyber incidents, while protecting their confidentiality and focusing on service recovery from such incidents. This paper explores the dilemma of information sharing versus sensitivity and provides a practical overview of considerations every business continuity plan should address to plan effectively for information sharing in the event of a cyber incident.

Keywords: cyber, threat, incident, information security, business continuity planning, intelligence, prevention, detection, response

INTRODUCTION

Cyber threats are growing and evolving at an unprecedented rate.[1] Rapidly evolving cyber criminal networks have already recognised the value of intelligence sharing and collaboration as evidenced by the growing number and sophistication of

Journal of Business Continuity & Emergency Planning
Vol. 7 No. 2, pp. 103–111

1749–9216

underground forums and information exchanges.[2] Government and industry information sharing is far less advanced. While organisations are beginning to recognise the imperative for cyber information sharing, they still face the challenge of balancing transparency and confidentiality.

This challenge is significantly increased given the growing interconnectivity between organisations and their partners; by way of example, it is increasingly common for attackers seeking sensitive information to target an organisation's supply chain (the attack vector being focused on a third-party vendor in order to reach the principal target). An example of such a data breach recently occurred at Bank of America, whereby attackers managed to successfully access employee and executive data stored through a third-party subcontractor.[3] What is particularly interesting about this attack is that it was allegedly motivated by a project initiated by Bank of America to monitor publicly available information in an effort to identify security threats.

The increasing complexity of supply chains coupled with the adoption of cloud-based services places greater onus on organisations to understand where their data are and to ensure that they are managed appropriately, in order to prevent suppliers' vulnerabilities from becoming their own. This further emphasises the importance of information exchange regarding cyber incidents within a supply chain.[4]

Commonality between cyber landscapes within organisations increases the appeal of exploiting shared weaknesses as malicious parties find cyber attacks that can be reused against multiple targets to be more attractive. Organisations and industries with mechanisms to disseminate information about cyber-attacks rapidly not only help others to minimise the impact from such incidents but also decrease the long-term attractiveness of themselves and their industry as targets.

Despite the challenges, organisations can take steps to enable their ability to share information before during and after cyber incidents, helping organisations and industries to build more resilient operating frameworks, while presenting themselves as less attractive targets.

PRE-INCIDENT DATA MANAGEMENT

Cyber incidents are increasingly expensive and prevention is better than cure.

Accordingly to a recent survey by the UK Department for Business, Innovation and Skills, the average cost of the worst security breach of the year is presently in the region of £450,000 to £850,000 and £35,000 to £65,000 for large organisations (>250 staff) and small business (<50 staff), respectively.[1] The report adds: 'in total, the cost to UK plc of security breaches is of the order of billions of pounds per annum — it's roughly tripled over the last year'.

Information can be used to enhance the organisation's ability to manage its data and its defences efficiently and effectively. Sources of information that an organisation can use as part of its incident management strategy can be varied, from independent sources of threat analysis (eg information related to tools, techniques and resources being used by attackers to breach cyber defences) and published industry-specific trends to third-party supplier/vendor reports of anomalies worthy of further review.[5]

Given the increasing dependence on third parties and growing inter-connectivity, organisations should consider adopting a more collaborative, 'partner' approach to incident management data exchange and analysis.

The business operating landscape is becoming more complex to manage

(especially with increasing outsourced dependencies). As a consequence, the challenge is to ensure that the organisation is capturing the right data and performing the correct levels of analysis. The term 'the right data' refers to information assets that assist the organisation in:

- identifying entities that may be targeting the organisation, their methods and their motivations;
- identifying emerging threats by analysis of industry sector/technical/supplier data;
- identifying, where possible, best practices and countermeasures to mitigate the threat.

Programmes designed to promote understanding of cyber risk, such as the Information Security Forum's Cyber Special Interest Group and the World Economic Forum's Partnering for Cyber Resilience,[6] provide useful data-sharing guidance by means of a common set of shared principles that organisations and their suppliers can agree upon and work to.

Small and medium enterprises increasingly face internal skills and resource challenges to effectively identify, assess and remedy cyber security risks. Resources such as the UK's Cyber-security Framework for Business[7] and IT Governance's Cyber Security Risk Assessment service[8] seek to promote good practice in this area.

Key questions to consider with regard to sharing cyber incident information include:

- What information needs to be shared?
- Where third-party vendor relationships are in scope, should formal agreements be put in place between important entities in order to establish the appropriate channels of incident management communication?
- When should information be shared?
- How will information be shared?
- Which information-sharing models are in scope during the pre-incident stage or business as usual?
- Has a decision-tree structure been defined to address any *ad hoc* data management or communication issues highlighted during an incident that require a timely response?

What information needs to be shared?

In the context of a service outage/emergency it may be that only a subset of data may be valuable to share. While it is understood that it would be impossible to anticipate all incident combinations, some preparatory investment with regard to important information requirements may save valuable time in the midst of managing an incident. By way of example, organisations should consider the consequences of information sharing and consistency of message approach. A recent online, phone and cashpoint service outage by the Royal Bank of Scotland Group led to a call for compensation by customers. One such case[9] resulted in the bank initially offering £30 to a customer for inconvenience/embarrassment caused, which was raised to £70 when he declined. News of the appeal success subsequently spread to social networks, whereby thousands of like-minded customers learned of the case and pushed for their own compensation payment increases. As a consequence, the original good intention of the bank to compensate customers could have potentially backfired due to a lack of planning. Agreeing a consistent information-sharing approach ahead of the incident could have potentially saved the bank additional negative publicity while promoting a fair and equitable process for customers. In order for incident management to be effective, collaboration with important

parties is essential; hence, communication and information sharing are required while being mindful of the need to know principles (particularly with regard to legal and privacy requirements). Prior consideration of these factors will save precious time in the midst of an incident.

Where third-party vendor relationships are in scope, should there be formal agreements between important entities to establish the appropriate channels of incident management communication?

By way of example, is there a requirement on third-party vendors to report security-related incidents and/or share specific incident data within an agreed period and format that would prove timely and cost-effective to the organisation? While organisations may not explicitly ensure that their third parties are subject to internal company control policies, there is potential to imply a consistent behaviour via a formalised agreement/contractual obligations. In order to maintain an acceptable level of expectation management, formal agreements should be in place to ensure that third parties have a tested and sufficient incident-response process including (but not limited to):

- the maintenance and communication of an up-to-date incident response plan;
- the definition of trigger points constituting a formal reporting requirement;
- incident reporting timeframes, format, communication channels and content;
- the disclosure approval process should the third party need to publish security breach information to an external party;
- participation in periodic drills, reviews, staff training and awareness.

When should information be shared?

Although this paper considers information sharing in three distinct phases (pre, mid and post-incident), organisations should consider in advance whether information will be shared on an ongoing transfer basis (in case it is required should an incident occur) or shared only in the event of pre-defined incident triggers (ie in response to specific events)?

Taking the above areas into account and by way of example, sharing intrusion attempt information could be disseminated quickly to predefined parties on the basis that:

- timely dissemination of intrusion attempt data provides valuable awareness for organisations;
- such data may be shared relatively swiftly as they require less sanitisation/analysis than other data sources;
- sharing attempted intrusion data does not reveal any significant detail concerning the reporting organisation's security posture other than its detection of the attempt (ie it does not reveal whether the reported attempt was successful).

How will data be shared?

All organisations should consider how they will share data, before during and after incidents. This should include whether the security of transmission (ie how data will be exchanged between parties) and access control have been acknowledged in establishing the data-sharing protocol at each stage.

If there is a requirement for incident data to be preserved for post-incident investigation and/or legal requirements, consideration as to how such data will be stored and retained should be in scope.

Which data-sharing channels are in scope during the pre-incident/ business as usual stage?

The effective deployment of data-sharing

sources and channels can enable an organisation to develop and enhance its cyber incident management strategies. Sharing between organisations can enable participants to develop tailored strategies. Common approaches to information exchange include the following:

- Pre-established forums (hub and spoke), which provide additional degrees of data analysis/provenance, correlation and source anonymity. The Warning, Advice and Reporting Point (http://www.warp.gov.uk) structure as provided by the Centre for the Protection of National Infrastructure is an example of a structured hub and spoke model. In addition, a number of industry-specific forums exist to provide incident-related data. By way of example, the Aviation Safety Information Analysis and Sharing system[10] is focused on the sharing of data from airlines to improve air safety. A centrally managed information hub receives information from multiple airlines and the Federal Aviation Administration. The resiliency of such exchanges, timeliness of content availability and performance/scalability limitations may need to be taken into account with regard to such solutions.
- 'Post to all' models, whereby organisations share information directly with a pre-defined membership. Maintaining a common taxonomy and preserving integrity of information content is important to the success of such trusted partner models.
- Larger organisations may engage in multiple information exchanges. Where this is the case, the challenge of adopting a standard approach to information sharing (eg common taxonomy, automation of processing) such that incident data may be prioritised and correctly acted upon is a potential area of focus.

Has a decision-tree structure been defined to address any *ad hoc* data management/communication issues highlighted during an incident that require timely response?

When an incident occurs, it is understood that the organisation's management will not have made decisions covering all eventualities. Having a pre-agreed decision structure in place prior to an incident will save an organisation significant time in the midst of managing an event.

This is an important area given the growth of social media adoption, whereby organisations should review their communications strategy with regard to incident management. This should be inclusive of clearance levels and escalation paths (ie who approves corporate messages to clients/external bodies?). Monitoring of social media feeds should also be considered to enable organisations to effectively manage their external profile. Companies such as Digital Shadows (http://digitalshadows.com/) provide monitoring, assessment and consultancy services to help address challenges in this area. Common issues related to social media (especially in the midst of an incident) include impersonation and the proliferation of misinformation. As such, organisations should be mindful of the need to adopt a communication strategy that seeks to address these emerging instances.

MID-INCIDENT DATA MANAGEMENT

Key questions to consider with regard to sharing information during a cyber incident include the following:

- What risk does data sharing pose?
- Will any sensitive data be transferred outside of the pre-approved boundaries?
- Are media channels being adequately managed?

What risk does data sharing pose?

Organisations must always consider whether the risk of sharing information is outweighed by the risk of not sharing it. One example of this is highlighted in the UK government report on lessons learned from the 7th July, 2005 terrorist attacks, which stated, '...in some parts of the emergency response, the requirements of the Data Protection Act were either misinterpreted or over-zealously applied',[11] which in turn led to a delayed emergency response. When assessing the risk, organisations should consider the potential impact of data sharing to individuals and organisations and individuals' trust in the organisations that keep records about them. In relation to this area, organisations may look to ask whether the incident management objective could be equally achieved without sharing the data in scope or by providing an anonymous cut of said data.

While the case for sensitivity and safeguarding confidentiality of data is often clear, these should be weighed up against the benefits of information sharing, particularly with regard to incident management, where timely access to such resources may significantly improve an organisation's capability to manage and even prevent attacks.

This is where time invested in identifying what types of data each organisation holds (and what is likely to be shared in the event of an incident) will pay off, resulting in a more efficient decision-making process in the event of a real incident.

Will any sensitive data be transferred outside of the pre-approved boundaries?

Organisations should consider guidance with regard to data protection and regulatory compliance in line with incident management, especially with regard to potential cross-border data access and transfer positions. By way of example, for organisations based in Europe, if there is a potential requirement for incident data to be transferred outside of Europe, the 8th Principle of the Data Protection Act would need to be considered.

Are media channels being adequately managed?

During an incident response when there is less time to consider issues in detail, it can be especially challenging to make judgments about whether specific information can be shared. Continuing to stay in touch with the media, checking whether messages concerning the organisation are in line and identifying when to intervene are important pillars of an effective communication strategy.

An increased dependency on shared/out-sourced services and the growth of social media solutions makes the management of sensitive data an even greater consideration.

A growing area of importance for media consideration is a review of the organisation's communication strategy to ensure a consistent approach. Monitoring of media sources to gather intelligence as well as placing a focus on controlling the formal messages disseminated via media channels (identifying any false reporting, which in itself can lead to incident escalation, while preserving the timeliness, accuracy and authenticity of communication[12] is a important factor to bear in mind.

The growing adoption of social media channels makes the above set of considerations a more challenging one given the complexity of the landscape, instantaneous broadcast and global reach capabilities. An important consideration is that of public trust levels. Levels of public unease and media attention naturally increase in the event of an incident. How organisations manage their communication strategy and

harness media channels will have a considerable impact on this area.

POST-INCIDENT DATA MANAGEMENT

Key questions to consider with regard to sharing information after an incident include the following:

- Have any data/information sharing mechanisms or channels established during the incident been restored to ensure that no subsequent data are being exchanged if it is no longer necessary to do so?
- Have appropriate controls been applied to safeguard incident data?
- What checks should be put in place to ensure that data sharing is meeting its defined objectives with regard to incident management?
- Has a post-incident 'lessons learned' review been carried out and have incident plans been updated where necessary to improve data management preparedness for future incidents?

Have any data/information sharing mechanisms or channels been restored?

It is important to consider recovery and restoration of data, access control and communication channels (eg where contingency channels were established for incident management purposes). All organisations should question whether these have been restored post incident to ensure that no subsequent data are being exchanged when there is no further requirement to do so. This would include the recovery and restoration of in-field incident kit, such as laptops, data drives, etc.

Have appropriate controls been applied to safeguard incident data?

Evidence may need to be retained, not only for post-incident review/investigation but also in light of any in scope legal requirements, whereby data may need to be preserved until all legal actions have been completed.

Incident data, which may initially appear insignificant, may subsequently become more important (eg if an attacker is able to use knowledge gathered in one attack to perform a more severe attack later) and evidence from the first attack may be important to explaining how the second attack was accomplished.

What checks should be put in place to ensure that data sharing is meeting its defined objectives with regard to incident management?

Both the organisation's operating model and risk landscape are constantly evolving. Hence, it is good practice to periodically monitor the effectiveness of any data-sharing strategy to ensure that the essential objectives of effective incident management are being met. Such a review could be part of a continuous improvement programme and address specific items such as whether it is still appropriate to share specific data and is there an appropriate balance between the sharing requirement and the risk?

Organisations should not underestimate the value of a post-incident 'lessons learned' review being carried out, inclusive of pre-incident plans being updated where necessary to improve data management preparedness for future incidents. Such reviews should ideally tie back into the organisation's policies and standards, plus training and awareness activities.

Post-incident data sharing initiatives to consider may also include the following:

- providing training on information handling to stakeholders to manage consistency of approach;
- creating a cyclical review mechanism to measure the effectiveness of the organi-

sation's incident data management model, review changes in the regulatory/operating environments and identify opportunities to refine;
- developing and communicating policy and guidance on information sharing and sensitivity to ensure compliance with regulatory requirements and objectives.

CONCLUSION

Given the evolving nature of attack vectors (a path or means by which an attacker can attempt to gain access to unauthorised network assets or the mechanisms through which organisations can be attacked) combined with the growing complexity of organisational dependency, an effective information-sharing strategy is not a one-size-fits-all approach. In many cases, a hybrid (best in class) approach may be appropriate to promote an agile information exchange solution.

Organisations seeking to set the right balance between information sharing and access control in the context of incident management should seek to apply proportionate levels of control over data sources, content and collection methods while respecting applicable regulatory and policy requirements on data use.[13]

In order to manage this objective more effectively, organisations should consider their respective data-sharing strategies as a live model. As attack vectors, business models and third-party dependencies evolve, there is a need for organisations to continually manage their incident management plans to ensure that they align to their operating environment and continue to remain effective as a result.

The areas discussed in this paper provide a common set of considerations for organisations to review when drafting and/or enhancing their respective incident management plans in order to more effectively achieve a sensible balance between information sharing and control.

REFERENCES

(1) Department for Business, Innovation and Skills/PWC (2013) 'Information Security Breaches Survey — Technical Report', available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/191670/bis-13-p184-2013-information-security-breaches-survey-technical-report.pdf (accessed 16th July, 2013).

(2) Marinos, L. and Sfakianakis, A. (2013) 'ENISA Threat Landscape — Responding to the Evolving Threat Environment', available at: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape (accessed 16th July, 2013).

(3) Integrity Research Associates (2013) 'Anonymous Hacks ClearForest', available at: http://www.integrity-research.com/cms/2013/03/05/anonymous-hacks-clearforest/ (accessed 16th July, 2013).

(4) Information Security Forum (2012) 'Securing the Supply Chain',

(5) Centre for the Protection of National Infrastructure (2013) 'Critical security controls for cyber defence — in depth', available at: http://www.cpni.gov.uk/advice/cyber/Critical-controls/in-depth/ (accessed 16th July, 2013).

(6) World Economic Forum (2012) 'Partnering For Cyber Resilience: Risk and Responsibility in a Hyperconnected World – Principles and Guidelines', available at: http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf (accessed 16th July, 2013).

(7) CESG (2012) '10 Steps to Cyber Security – Executive Companion', available at: http://www.bis.gov.uk/assets/BISCore/business-sectors/docs/0-9/12-1120-10-steps-to-cyber-

security-executive.pdf (accessed 16th July, 2013).

(8) IT Governance (2013) 'New service helps UK SMEs implement government's cyber risk guidance', available at: http://www.it governance.co.uk/media/press-releases/new-service-helps-uk-smes-implement-government%E2%80%99s-c.aspx (accessed 16th July, 2013).

(9) BBC Business News (2013) 'RBS to compensate customers after accounts disrupted', available at: http://www.bbc.co.uk/news/business-21694704 (accessed 16th July, 2013).

(10) Mitre Corporation (2012) 'Cyber Information-Sharing Models. An Overview', available at: http://www.mitre.org/work/cybersecurity/pdf/cyber_info_sharing.pdf (accessed 16th July, 2013).

(11) HM Government (2007) 'Data Protection and Sharing – Guidance for Emergency Planners and Responders', available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60970/dataprotection.pdf (accessed 16th July, 2013).

(12) KPMG (2012) 'The Social Banker – Social Media Lessons from Banking Insiders', available at: http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/social-banker/Documents/social-media-lessons-from-banking-insidersv3.pdf (accessed 16th July, 2013).

(13) The White House – Washington (2012) 'National Strategy for Information Sharing and Safeguarding', available at: http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf (accessed 16th July, 2013).