Contrasting Approaches to Incident Reporting in the Development of Safety and Security-Critical Software

Chris W. Johnson,

School of Computing Science, University of Glasgow, Glasgow, G12 8RZ.

Johnson@dcs.gla.ac.uk,
http://www.dcs.gla.ac.uk/~johnson

Keywords: Incident reporting, Safety Management Systems, Root Cause Analysis, Organisational Resilience

Abstract. There are increasing obligations on companies to report cyber-security incidents to national and international regulators. Article 13a of the Telecoms Directive (2009/140/EC) requires network service providers to report significant security breaches and losses of integrity to competent national authorities. The United States Security and Exchange Commission also expects its members to file information about cyber incidents. Existing cyber-incident reporting systems, typically, use tools and techniques that were initially intended to support Safety Management Systems, including reconstruction and causal analysis. This unified approach is particularly useful when, for example, the consequences of a cyber attack might compromise safety. In contrast, this paper identifies differences that complicate the use of conventional safety reporting techniques to mitigate cyber threats. For instance, it is important to communicate safety lessons as widely as possible to avoid any recurrence of previous accidents. However, disclosing the details of a security incident can expose vulnerabilities or assets that motivate further attacks. Similarly, most safety-management systems have clear reporting mechanisms via industry regulators. This is far more complicated for security incidents where companies have to report both to national industry regulators and to national telecoms authorities. They may also have to contact local and national law enforcement, to Computer Emergency Response Teams (CERTs) and to national infrastructure protection agencies. At a more technical level, the counterfactual arguments that are often used to distinguish causes and contextual factors in safety related accidents cannot easily be used to reason about the malicious causes of security incidents. The closing sections of this paper propose a research agenda that is urgently required before the proposed EC Network and Information Security Directive (COM2013/48) extends the Article 13a reporting obligations across all European critical infrastructure providers.

1 Introduction

The EU Telecoms directive (2009/140/EC) places an obligation on the providers of networks and services to manage security risks and to take appropriate measures to guarantee the security and integrity of their operations. In particular, Article 13a requires providers to report significant security breaches and losses of integrity to competent national authorities. The proposed Network and Information Security Directive extends this obligation to 'market operators' responsible for critical national infrastructures, across the energy, banking, health, transport, financial services and food sectors. These initiatives mirror trends in the United States, where for example the Security and Exchange Commission already expects its members to file information about cyber incidents, which are "significant factors that make an investment in the company speculative or risky". In consequence, many organizations are establishing reporting systems for gathering information about cyber-incidents. These initiatives typically build on reconstruction, causal analysis and pattern matching techniques that were initially intended to support existing Safety Management Systems [1].

In contrast, this paper identifies differences that complicate the use of conventional safety reporting techniques to mitigate cyber threats. For instance, it is important to communicate safety lessons as widely as possible to avoid any recurrence of previous accidents. However, disclosing the details of a security incident can expose vulnerabilities or assets that motivate further attacks. Further insights include the need to unify cyber-reporting mechanisms – in some sectors companies must report to industry regulators, to national telecoms agencies, to local and national law enforcement, to Computer Emergency Response Teams (CERTs), to national infrastructure protection agencies. In contrast to more established safety-reporting systems, these different security reporting schemes have inconsistent data and disclosure requirements. Their utility is further undermined by the lack of data mining or other information retrieval tools that might be used to identify common attack patterns on software used both within and across critical infrastructures. Other concerns focus on the need for companies to secure their supply chain – especially where they may not know about the COTS products being used by sub-

contractors within their own facilities. Following a safety-related incident, sub-contractors will often work closely with service providers to identify and rectify potential problems. The safety-maturity level of most organizations is usually more developed than any comparable security culture. In consequence, the response to security related incidents is often to deny responsibility and avoid blame [2]. This compromises the utility of incident reporting when commercial confidentiality and IP barriers frustrate attempts to diagnose the vulnerabilities that compromise cyber-security.

2 Adapting Safety Management Systems to Cyber Reporting

Incident reporting systems are an important component of safety-management systems [3]. They provide information about hazards that were not identified during the early stages of design. They can also provide important insights into hazards that were identified but that were not adequately mitigated during the design and implementation of safety-critical software. These schemes have been used to improve safety across many industries – including the UK Confidential Reporting Programme for Aviation and Maritime (CHIRP), the European Railway Agency harmonised reporting systems and the Safe Work Australia tools for the process industries. Initially, most systems were voluntary. However, recent years have seen the development of compulsory reporting infrastructures, following the model embodied within Article 13a or the US SEC requirements. A range of international reporting system,s have also been established to support the exchange of safety-related information. For example, EUROCONTROL has developed a number of techniques to ensure the exchange of safety-related information in Air Traffic Management between member states, see for instance the sections on degraded modes for software on http://www.skybrary.aero. These diverse applications share safety insights between many different stakeholders; including operators, suppliers, regulators, safety managers, accident investigators etc.

The perceived success of incident reporting systems in safety-critical industries has inspired a number of organisations, including the US National Institute for Standards and Technology (NIST) and the European Network and Information Security Agency (ENISA) [4], to develop similar infrastructures to gather information about cyber-security incidents. There are similar motivations for incident reporting within both safety and security management systems. Risk assessments help to identify the potential targets of an attack and to determine whether there are known vulnerabilities. Security measures are then taken to protect those targets and to ensure that measures continue to be implemented over time. Incident reporting systems provide important feedback on the strengths and weaknesses of these security measures.

The insights from a cyber-security incident reporting system help to focus and justify subsequent investments. Just as in safety, considerable resources can be deployed to address threats that are never realised. In such circumstances, without evidence of attacks or of safety incidents in other organisations, management can be under pressure to cut safety and security budgets. Incident reporting can; therefore, help to validate security threat analysis and safety risk assessments.

The US Department of Homeland Security (DHS) National Cyber security and Communications Integration Center (NCCIC) coordinates the collection and dissemination of threat information. The NCCIC uses this data to improve situation awareness across public and the private organisations. Increasing national resilience and informing longer-term threat assessments. They also disseminate information to coordinate the national response to any attack.

There are further long-term motivations behind the development of cyber incident reporting systems. In particular, there have been moves in Europe and North America to develop a cyber insurance market that enable companies to offset an element of the risk of future attacks. They cannot easily quantify the risk of any future attack hence they seek to offset first and third party costs using insurance. However, the actuaries and under-writers have traditionally adopted a cautious approach charging high premiums for this form of cover given the problems of risk quan-

tification. The Obama administration has recently considered tax breaks to encourage companies to invest more in cyber-security. A limit on liability has also been proposed; this reduces the cost of cyber-insurance because under-writers can be sure of the upper limit of their exposure for each claim based on the existing Terrorism Risk Insurance Act (TRIA). However, these and similar proposals in Europe pioneered by ENISA, have been linked to compulsory cyber incident reporting requirements so that insurance companies can accurately assess the frequency and consequence of previous attacks on similar organisations when calculating their premiums.

3 Integrating Safety and Cyber Security Reporting Systems

There have been few attempts to integrate safety and security reporting systems. One reason for this is a traditional distinction between the safety and security teams in software-related organisations. They follow different standards – typified in the distinction between the ISO 27k security series and IEC61508 in the process industries. Although there are common concepts, such as risk assessment and mitigation, the detailed definitions and the techniques used to perform similar tasks can be very different.

This is lack of integration raises significant concerns given that safety-critical systems are increasingly vulnerable to cyber attacks [5, 6]. In the past, safety related applications were hard to attack because few people had the technical skills necessary to identify vulnerabilities in bespoke operating systems and network protocols. In contrast, many industries now rely on Commercial Off-The Shelf (COTS) infrastructures, including Linux and the IP stack.

There are three main cyber threats to safety-critical infrastructures. The first stems from disaffected insiders. Companies increasingly rely on a wider range of sub-contractors with correspondingly less knowledge of their underlying technical infrastructures. Incident reporting is important because it can help national security agencies and regulators to determine the extent of this problem and identify changes over time, for instance the growing use of service oriented service provision.

A second source of attack is from the creators of mass-market malware. These attackers typically have little interest in safety-related applications. Instead, their focus is on intercepting credit-card details or account passwords. They are not trying to halt electricity generation or aviation operations. These attackers have little idea of the impact their code can have on safety-related systems. For example, 'second generation' denial of service attacks force operators to suspend critical processes following the detection of mass-market malware. It is unlikely that the development techniques used to create a Trojan would meet the requirements of an industry regulator within safety-critical industries!

Finally, a growing number of attacks and of active surveillance programs stem from state sponsored agencies. The detection of W32.Stuxnet and its predecessors has shown what is possible. Sniffer applications, which exfiltrate network and infrastructure information, have been found in national critical infrastructures. It is, therefore, important that we learn as much as possible from previous cyber-attacks, not only those that are intended to inflict direct, deliberate damage but also those that disclose sensitive information that compromise the longer-term safety of complex systems.

In previous work, with support from ENISA, we have identified a range of techniques that can be used to integrate safety and security incident reporting [2]. There are a number of motivations for this. The most obvious is to reduce the complexity of maintaining two orthogonal reporting architectures. This has implications for reporting bias when staff are unsure how to submit to either system. In many cases, it can be difficult to determine whether an incident has been triggered by a more routine software bug or by a deliberate attack – especially given that the state machine used to drive the Stuxnet attack was deliberately intended to mask the attack as a PLC-STEP 7 software failure.

Different architectures have been developed to support the integration of safety and cyber-security incident reporting [2]. Company reporting systems have been established to collate manual submissions or the results of automated anomaly detection. Incident investigators gather further evidence, including system logs, to map out the events leading to an in-

trusion or safety concern. Reconstruction and analysis support more detailed studies of the causal and contributory factors. From there it is possible to identify those actions, which are intended to reduce the likelihood or mitigate the consequences of any recurrence. The findings are then distributed to other stakeholders within the organisation so that corrective actions can be implemented.

Internal safety and security reporting systems have a number of limitations. The corrective actions often focus on disciplining staff rather than on identifying underlying causes – such as inadequate procedures or training. Internal reporting systems also limit the dissemination of security information across an industry. In consequence, the Telecom Directive and the proposed EC Network and Information Security Directive introduce interfaces between internal security reporting systems and external organisations just as existing regulatory provisions, such as the European Railway Safety Directive (2008/110/EC) create interfaces for the exchange of safety related information.

4 Differences between Safety and Cyber Security Reporting

The previous section has identified the concerns that motivate the integration of reporting systems for gathering information about safety and cyber security concerns. However, the following paragraphs identify a host of differences that complicate the development of common approaches. This paper is the result of having helped in the design and implementation of reporting systems across a number of industries – including the ENISA reporting system fro Article 13a and commercial systems run by energy distribution companies as well as several European Air Navigation Service Providers. Confidentiality concerns prevent direct references to the architecture of particular systems and this in itself illustrates both the sensitivity of security incident reporting tools and also the need to identify an appropriate security culture to match the safety culture that enables the exchange of information that can help avoid future accidents.

4.1 The Imbalance between Safety and Security Incidents

One of the most striking differences is the relative frequency of safety and security concerns that are submitted to integrated reporting systems. Typically, cyber security reporting functions are later added to an existing safety management system. Most reports focus on safety concerns. One interpretation is that safety-related organisations suffer a comparatively low level of security incidents. Alternatively, it can be argued that the imbalance reflects a reporting bias – with staff either failing to detect or deliberately not submitting cyber security reports. Further work is required to investigate these different hypotheses. Until then, it seems likely that the reporting imbalance stems from a mixture of these concerns. Management implicitly improve many security violations, for example the use of USB devices by sub-contractors, because they are anxious to maintain operations. These incidents would not normally be reported even though they threaten the integrity of an infrastructure. At the same time, many safety-related systems lack automated intrusion detection that might identify potential malware – this is particularly true for SCADA systems using PLCs and Smart Controllers where these are very limited forensic tools.

The relatively low frequency of cyber-security incidents in safety-related industries has a number of knock-on consequences for security management systems. Many companies lack the specialist forensic resources to identify the causes of a cyber attack. In internal resources must be supplemented by external expertise from national CERTs, regulatory agencies or industry associations. In practice, this implies a loss of control and an admission that the company cannot cope on its own. The loss of control and the reliance on external agencies can also compromise intellectual property where investigators must be familiar with commercially sensitive information in order to diagnose the causes of an attack. In consequence, there are significant incentives for companies NOT to report cyber-security concerns when in most cases the standard internal debugging and maintenance processes would be sufficient to address most mainstream safety concerns. Either, companies must trust the external agencies they rely on during any crisis. Or legislation must persuade companies to seek external support when potential attacks are

identified against critical infrastructures. The US Federal Communications Commission has levied punitive fines on those companies that have been shown not to report similar incidents through their NORS and DIRS reporting infrastructures.

4.2 The Threats from Dissemination

The exchange of information about a safety-related incident is normally intended to prevent any recurrence. A strong safety culture helps to ensure that recommendations are widely distributed and that the focus of any findings identifies appropriate mitigations rather than seeking to blame individuals or organisations. In contrast, the dissemination of lessons learned might increase the likelihood of future cyber attacks by helping attackers identify previous vulnerabilities that have not been corrected across all of the systems operated by the victim. Reports about the causes of a breach will also expose the systems operated by other organisations that remain to be patched. Information about the remedial actions taken after a security incident can also provide insights into future vulnerabilities of a previous target. It is for this reason that many organisations operate closed or internal reporting architectures; where information is only intended to be shared with others inside that company.

Inside the company, safety and security management groups provide an interface between the team running the reporting system and external agencies, including national regulatory bodies, industry associations, CERTS and national security agencies. The management group plays a critical role in the success of the reporting system; many companies are reluctant to provide their competitors with a commercial advantage by disclosing information about previous attacks. There are justified concerns about the potential impact of disclosure on market confidence and on potential litigation. Without legal protection, many companies only provide anonymous summaries security incidents, especially if they have a potential impact on safety.

The sensitivity associated with cyber incident reporting, typically, imposes significant additional security constraints in terms of the minimal access controls that are typify many safety-reporting systems, especially

during the dissemination phase. In particular, there is often a need to create 'case study' documents that capture the essence of an attack and maintain the confidentiality of the victim without providing the technical details that would be required to launch a future attack. This can leave Chief Information Security Officers and their teams feeling frustrated when they cannot glean sufficient information to directly protect their systems from the generic lessons that are published by security reporting systems. Further work is urgently required to identify appropriate levels of abstraction that can be used to protect future systems without publicising existing vulnerabilities to potential attackers.

4.3 Conflicts of Notification

One of the most immediate concerns from the integration of safety and cyber-security reporting systems is to determine the appropriate interfaces with external agencies that must be notified after an incident has occurred. It can be unclear whether reports should be sent to an industry regulator, such as the US Federal Aviation Administration or Nuclear Regulatory Commission, to a security agency, such as the Department of Homeland Security or the US CERT, or to telecoms regulators who have responsibility for collating information about wider cyber-security concerns such as the Federal Communications Commission. In some cases, a single incident must be reported to more than one agency. For example, a cyber-attack with safety related consequences must be reported to the national industry safety regulator and potentially also to a subset of the National Crime Agency, the National Cyber Crime Unit, GOVCERT, the UK Information Commissioner as well as the CESG/Centre for the Protection of National Critical Infrastructure via providers registered under the Cyber Incident Response (CIR) or the Cyber Security Incident Response Scheme (CSIR). There is widespread confusion over who to consult. In the United States, there are Federal investigatory agencies (e.g., the Federal Bureau of Investigation [FBI] and the U.S. Secret Service), district attorney offices as well as both state and local (e.g., county) law enforcement. Regulatory agencies introduce an additional layer of complexity in safety-related industries. It is for this reason that NIST urge organisations to contact the legal agencies that must respond to cyber incidents; "one reason many security-related incidents do not result in convictions

is that some organizations do not properly contact law enforcement... incident response team should become acquainted with its various law enforcement representatives before an incident occurs to discuss conditions under which incidents should be reported to them, how the reporting should be performed, what evidence should be collected, and how it should be collected" [7].

The main distinction between these different systems is that some explicitly understand the safety-related domain in which an incident occurs but have little cyber security competence while others have little or no industry specific safety-related competence but do understand the general class of cyber-threats. In particular, industry safety regulators have almost no expertise in cyber-security; many suffer from a long legacy of physical security specialists whose talents provide little help in mitigating new generations of advanced persistent threats. These problems have been recognised, for example in recent reports from the US Government Accountability Office: "A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges" [8] and "Cyber security: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented" [9]. There is a need to draft letters of agreement between regulatory and state security agencies to establish roles and responsibilities in the aftermath of a cyber-attack. These help to avoid "turf wars" when engineers are working to ensure the safety of compromised systems.

These conflicts and confusions between safety and security lines of reporting are compounded because many companies operate across national borders. Each local division must respect the very different reporting mechanisms and jurisdictions that have been implemented in each country. There are further complexities, especially in Europe where there are increasing requirements to report to national agencies and also to share recommendations with other member states, for example within the proposed Network and Information Security Directive. If an incident is detected in a system in one national jurisdiction, there is often a requirement to share lessons with groups in other countries without compromising national sovereignty in any area of operation. Appropriate

means of achieving this remain the subject both of academic research and of heated debate within the European Commission [9].

4.4 Different Legal Contexts

Further problems complicate the integration of safety-critical and cyber security reporting systems. In safety-related incidents, investigators are guided by general requirements to gather sufficient evidence to reconstruct the context in which an incident occurred. For instance, in aviation this is governed by the ICAO International Standards and Recommended Practices (SARPS) contained in the nineteen Technical Annexes to the Convention on International Civil Aviation. In particular, Annex 13 deals with Aircraft Accident and Incident Investigation – the clauses dealing with the preservation of evidence make it clear that an investigator must notify state security agencies if they believe that material has been tampered with. In contrast, companies must be aware of the more detailed judicial and legal requirements when conducting forensic investigations [10, 11]. The systems and networks that are affected by a suspected cyber-attack can be considered a crime scene and evidence must be preserved according to legal principles preserving the chain of evidence. It will be necessary to uncover normal, hidden, deleted, encrypted and password-protected files to gain as much information as possible about the nature and scope of any attack.

The legal and regulatory framework for the investigation of cyber incidents is likely to become more and more complex with the increasing cross-border integration of national critical infrastructures. The European Commission has encouraged the interoperability of national rail networks. They have promoted the development and integration of smart grids and the creation of the single European skies network. We have already glimpsed the confusion that this can create in the investigation of conventional system failures, including the Viareggio accident that has taken years not months to complete. The US Department of Justice makes it clear that the web of international interdependencies is far more complex in cyber incidents, for example when a company in one country is attacked through the exfiltration of operational data on servers in a se-

cond state that are attacked by systems in a third nation remotely controlled by attackers in a fourth state [12].

In the UK, the Association of Chief Police Officers [13] has published guidelines for the handling of evidence following cyber incidents:

1. No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court;
2. In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions;
3. An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result;
4. The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

These principles were drafted to support cyber incidents in 'conventional' or office-based systems. They do not address the conflicts between a desire to meet forensic guidelines and the need to maintain levels of safety and levels of service. In practice, it is likely that senior investigators will have to work closely with systems and safety engineers. We urgently need more guidance on the roles and responsibilities of these key staff in the aftermath of cyber incidents affecting safety-critical infrastructures [14]. The US Department of Justice [12] reinforce these arguments when they suggest that first responders must:

- "Immediately secure all electronic devices, including personal or portable devices.
- Ensure that no unauthorized person has access to any electronic devices at the crime scene.
- Refuse offers of help or technical assistance from any unauthorized persons.
- Remove all persons from the crime scene or the immediate area from which evidence is to be collected.
- Ensure that the condition of any electronic device is not altered.

- STOP! Leave a computer or electronic device off if it is already turned off".

It would be hard to enforce such cyber-incident response requirements in safety-critical systems. Removing "all persons from the crime scene" could be catastrophic in a crowded Air Traffic Control centre or Nuclear control room where recovery from a cyber-incident requires cooperation between multiple teams. To "leave a computer or electronic device off if it is already turned off" would prevent the use of redundant protection systems. Such conflicts illustrate the hose of legal and forensic concerns that stem from the integration of cyber and safety related reporting requirements.

4.5 Concerns over Causal Analysis

In safety-critical systems, there has been a growing focus on the systemic factors that create the context in which an incident or accident is likely to occur. In contrast, security investigations tend to focus more narrowly on the policies and procedures that have been violated as a precursor to an incident. There is often a disciplinary aspect to the causal analysis that is less apparent in the immediate aftermath of safety related events. This difference between safety and cyber-security incident reporting can be explained in terms of the links between cyber-security, physical security and policing associating blame with legal transgressions. There are other potential interpretations. The differences in causal analysis and in recommendations between safety and security incidents may be due to the relative maturity of the two areas. Most security reporting systems are being integrated with existing safety management systems. The perfective approach focussing on the attribution of human error in previous generations of safety reporting is still to be seen in the relatively immature field of security investigation. In this interpretation, we might expect that the focus of security investigations may shift over time from individual violations to systemic factors through development in the underlying 'security culture'. Irrespective of the reasons behind these differences, questions remain about the tools and techniques that investigators might use to improve the coherence and consistency of causal analysis in the aftermath of cyber incidents. In particular, further work is re-

quired to determine whether the existing application of safety-related root cause analysis techniques, including those using counter-factual reasoning and systemic models, can be extended to support the analysis of cyber-attacks [3]. For instance, it is hard to be sure that any security measures in isolation will be sufficient to have prevented a directed intrusion – especially when we cannot be certain that we have detected all active malware in the aftermath of an attack.

4.6 Conflicting Recommendations in Security and Safety Reporting Systems

A final area of concern illustrates both the need for integration between safety and cyber-security incident reporting as well as the technical problems in achieving this integration. Many existing safety recommendations create security vulnerabilities and vice versa. As a specific example, redundancy is typically used to increase the dependability of critical systems. However, this provides few benefits in software related systems without some level of diversity. Leaving aside the issue of common requirements failure, two redundant versions of the same code are likely to contain the same bugs and hence fail in the same way. In consequence, N-version programming techniques rely on using two or more teams/contractors to develop redundant versions of the same program. In the event of one program failing, it is hoped that the diverse supply chain used to deliver the redundant version will ensure that they do not share common bugs. This approach to safety-critical software development has been widely accepted and used, for instance in the deployment of Air Data Inertial Reference Units across most commercial aircraft. Unfortunately, such techniques create immediate problems for security management. Companies must devote considerable expense to security two diverse supply chains – increasingly this involves audit processes to ensure that sub-contractors meet agreed security policies during the development of diverse, redundant code. In the past, these security concerns were not factored in the costs associated with such safety-critical software development practices.

A converse set of problems arises from the introduction of intrusion detection systems in the aftermath of security related incidents. White list approaches create problems because in most safety-related systems the

use of sub-contractors and significant legacy systems prevents operators from enumerating all of the processes that should be running within a particular application. Conversely, there are concerns over black-list approaches because the malware signatures that are downloaded every 24 hours in most desktop systems might themselves cause a safety related system to fail – and cannot be subjected to the extensive verification and validation processes recommended by safety related standards without creating a lengthy delay during which the application process would be unpatched and vulnerable to any attack. Alternatives such as the use of data diodes that enable monitoring of intrusions without altering network traffic raise further questions when false positives force the closure of safety-related services[1]. The meta-level point is that integrating safety and security critical computation reveals a host of tensions, which can only be addressed through integrated research in venues such as SAFECOMP.

5 Conclusions and Further Work

This paper has identified a number of national and international initiatives that extend reporting requirements from safety related events to include cyber-incidents. Attempts have, therefore, been made to integrate security events into existing safety reporting architectures. This is motivated by superficial similarities in terms of the processes involved in recording and analysing these incidents. In both safety and security, it is important to obtain 'sufficient' evidence, to reconstruct an adverse event, to conduct causal analysis, to identify corrective actions etc. Many of these tasks are already well supported within safety management systems. However, it is important to recognise that malware also poses some unique challenges – for example, the forensic analysis of a cyber-attack is very different from most accident investigations. An active adversary will deliberately seek to disguise their actions. Further complexities stem from the need to safeguard an application and the public in the immediate aftermath of a cyber attack. For instance, how do we land the aircraft

[1] These issues are addressed in a companion paper submitted to SAFECOMP on Barriers to the Use of Intrusion Detection Systems in Safety-Critical Applications.

in flight when we fear that an Air Traffic Management infrastructure is compromised and yet at the same time meet legal requirements to safeguard forensic evidence?

This paper has argued that to address such questions, we must encourage the integration of expertise across both safety and security management. In particular, we must identify appropriate communications interfaces with both internal and external stakeholders – to establish clear jurisdictions, roles and responsibilities. There is significant scope for further work. In particular, tools and techniques are urgently required to support the safety analysis of security incidents and vice versa. This is particularly important given that most safety-critical companies lack in-house forensic expertise. As mentioned, gathering evidence in the aftermath of a security incident poses unique challenges within safety-critical applications [2]. Existing guidance from the US Department of Justice focuses on conventional office based systems. They stress the need to isolate compromised networks both to preserve evidence and to prevent cross-contamination. Such guidance cannot easily be applied in many safety-critical systems when, for instance, passengers and aircrew rely on continued service from air navigation service providers. Additional support is also required for the causal analysis of security incidents; in safety-related systems there has been a focus on systemic approaches that look for the detailed managerial and organisational precursors to accidents and incidents. These ideas have had little impact on security management where many recommendations continue to focus on the immediate violation of rules and regulations by operational staff.

6 References

1. C.W. Johnson, Supporting the Exchange of Lessons Learned from Cyber-Security Incidents in Safety-Critical Systems. In D. Swallom (ed.), Proceedings of the 32nd International Systems Safety Society, Louisville, International Systems Safety Society, Unionville, VA, USA.

2. C.W. Johnson, Inadequate Legal, Regulatory and Technical Guidance for the Forensic Analysis of Cyber-Attacks on Safety-Critical Software. In D. Swallom (ed.), Proceedings of the 32nd International Systems Safety Society, Louisville, International Systems Safety Society, Unionville, VA, USA.

3. C.W. Johnson, Failure in Safety-Critical Systems: A Handbook of Accident and Incident Reporting, University of Glasgow Press, Glasgow, Scotland, 2003.

4. NIST, Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-61 Revision 2, August 2012.

5. C.W. Johnson, CyberSafety: On the Interactions Between CyberSecurity and the Software Engineering of Safety-Critical Systems. In C. Dale and T. Anderson (eds.), Achieving System Safety, 85-96, Springer Verlag, London, UK, Paper to acompany a keynote address, 20th Annual Conference of the UK Safety-Critical Systems Club, ISBN 978-1-4471-2493-1, 2012.

6. C.W. Johnson, The Telecoms Inclusion Principle: The Missing Link between Critical Infrastructure Protection and Critical Information Infrastructure Protection. In P. Theron and S. Bologna (eds.), Critical Information Infrastructure Protection and Resilience in the ICT Sector, IGI Global, Pennsylvania, USA, 2013.

7. U.S. National Institute of Standards and Technology (NIST) (2006), Guide to Integrating Forensic Techniques into Incident Response, Special Publication 800-86, Gaithersburg, Maryland, 2006. http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

8. US Government Accountability Office, A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges, GAO-13-462T, Washington, DC, USA. March 7, 2013

9. US Government Accountability Office, Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented, Washington, DC, USA, GAO-13-187, February 14, 2013.

10. U.S. National Institute of Standards and Technology (NIST) (2006), Guide to Integrating Forensic Techniques into Incident Response, Special Publication 800-86, Gaithersburg, Maryland, 2006. http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

11. U.S. National Institute of Standards and Technology (NIST) (2012), Computer Security Incident Handling Guide (Draft), Special Publication 800-61 Revision 2 (Draft), Gaithersburg, Maryland, 2012. http://csrc.nist.gov/publications/drafts/800-61-rev2/draft-sp800-61rev2.pdf

12. U.S. Department of Justice (2004), Forensic Examination of Digital Evidence: A Guide for Law Enforcement, 2004.

13. Association of Chief Police Officers (2011), Managers Guide: Good Practice and Advice Guide for Managers of e- Crime Investigation, 2011, ACPO. http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf

14. C.W. Johnson, Inadequate Legal, Regulatory and Technical Guidance for the Forensic Analysis of Cyber-Attacks on Safety-Critical Software. In D. Swallom (ed.), Proceed-

ings of the 32nd International Systems Safety Society, Louisville, International Systems Safety Society, Unionville, VA, USA.