scripted

Volume 13, Issue 3, December 2016

INCIDENT RESPONSE: PROTECTING INDIVIDUAL RIGHTS UNDER THE GENERAL DATA PROTECTION REGULATION

Andrew Cormack[*]

Abstract

Identifying and fixing problems with the security of computers and networks is essential to protect the data they contain and the privacy of their users. However, these incident response activities require additional processing of personal data, so may themselves create a privacy risk. Current laws have created diverse interpretations of this processing – from encouragement to prohibition – creating barriers to incident response and challenges for collaboration between incident responders. The EU's new General Data Protection Regulation explicitly recognises the need for processing to protect the security of networks and information. It also, through rules on processing for "legitimate interests", suggests a way to identify an appropriate balance between risks. Consistent use of these provisions could provide a common legal approach for incident response teams, enabling them to work more effectively. This article builds on analysis by the Article 29 Working Party to develop a framework for assessing the benefit and impact of incident response activities. This is applied to a range of practical detection, notification and information sharing techniques commonly used in incident response, showing how these do, indeed, protect, rather than threaten, the privacy and data protection rights of computer and network users.

DOI: 10.2966/scrip.130316.258

[*] Chief Regulatory Adviser, Jisc Technologies.

1. Introduction

Failures of computer security are among the greatest threats to privacy and data protection in the twenty-first-century. Recent news stories include twenty-one million people's security vetting records being exposed by a security breach at the US Office of Personal Management,[1] more than a hundred million LinkedIn user passwords being offered for sale,[2] and six million compromised PCs joining the Necurs botnet.[3] Victims of these, and many other, incidents have had sensitive data (including health and financial) disclosed, may have lost control of their professional networks (and any other services where they used the same password), or have an intruder controlling their computer and any systems they access from it. It is unlikely that these individuals could have detected these incidents themselves: data and password breaches happen on systems managed by other organisations, and malicious software hides itself from local users. External incident response teams, who monitor systems and networks to detect security problems and manage their mitigation, are an essential protection measure.

However, the work of incident response teams also represents a privacy risk. To detect incidents they must gather and process data about normal and abnormal activity on networks and computer systems, and share their findings with affected system owners and other teams. Inappropriate disclosure or use of this information could harm both the privacy of users and the security of systems. Teams must ensure the benefit from their activities is greater than the risk. European law, which regards both privacy and data protection as fundamental rights, ought to support this work, but national laws and interpretations are often unclear and inconsistencies create barriers, especially for cross-sector and international cooperation. These obstructions to detecting and responding to incidents are likely to increase their impact. The EU's new General Data Protection Regulation ("Regulation") offers two opportunities. First, it offers a clearer and more consistent legal approach across Europe. Second, it offers explicit recognition of "ensuring network and information security" as a "legitimate interest" of:

> public authorities, … computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), … providers of electronic communications networks and services and … providers of security technologies and services.[4]

And, it might add, of their users and data subjects.

---

[1] R Jalabi, "OPM Hack: 21 Million People's Personal Information Stolen, Federal Agency Says" (2015) available at https://www.theguardian.com/technology/2015/jul/09/opm-hack-21-million-personal-information-stolen (accessed 27 Nov 16).

[2] D Beres, "LinkedIn Users Might Want To Change All of Their Passwords ASAP" (2016) available at http://www.huffingtonpost.com/entry/linkedin-hack-change-password_us_573f2865e4b00e09e89ece22 (accessed 27 Nov 16).

[3] BBC, "Huge Spam and Malware Network Goes Offline" (2016) available at http://www.bbc.co.uk/news/technology-36519044 (accessed 27 Nov 16).

[4] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, Recital 49.

This article first discusses the need to prevent, detect and remedy security incidents, and the different types of data processing these involve. It then reviews the diverse treatment of these activities under existing laws and the difficulties this has created. In search of a more consistent alternative, following the lead of the Regulation, it considers the legal requirements and guidance when processing personal data for legitimate interests, concluding that existing incident response practice largely satisfies them. From these requirements and guidance it derives a framework to guide the work of incident response teams and applies this to common incident response activities.

2. How Incident Response Protects Data and Privacy

> [T]he effective protection of ICT systems from any attacks or illicit interception is essential to protect the fundamental rights to privacy and to data protection of individuals in the EU.[5]

Both privacy and the protection of personal data are considered fundamental rights in European law. Article 7 of the Charter of Fundamental Rights of the European Union[6] requires "respect for private and family life, home and communications"; Article 8 requires that personal data be protected and only processed when fairness and law permit. Personal data and communications are frequently held on computers and transmitted over electronic networks between them, so any weakness in the security of these systems creates a risk that both rights will be infringed: that communications and data will be observed or processed by unauthorised people or organisations. This may be most obvious when databases of personal information are compromised and made available to others but worse, and longer-lasting, damage can result from revealing your password to a phishing attack or having a malicious website or e-mail install malware on your PC. An intruder with control of a computer can see everything its legitimate users can, read all their files and track everything they do. Login details let criminals empty bank accounts or commit other frauds in the legitimate user's name. Loss of control on this scale clearly represents a serious compromise of both rights. The best way to protect rights is to prevent such incidents: when they happen, prompt detection and mitigation can limit the damage.[7] Lessons learned during mitigation can inform future preventive measures.

Security incidents are rarely visible to their victims until significant harm is done. Attackers modify the computers they compromise to make their presence invisible; the fact that someone has access to sensitive personal information may only become apparent when that information is published or otherwise misused. However, external observers may be able to detect signs and provide warnings before these damaging consequences occur. Unusual patterns of activity are more obvious given a wide view of what is normal, and such traces are harder for attackers to conceal.

---

[5] European Data Protection Supervisor, "Opinion 8/2015 Dissemination and use of intrusive surveillance technologies" (15 December 2015).

[6] *Charter of Fundamental Rights of the European Union* (2012/C 326/02).

[7] ENISA, "Actionable Information for Security Incident Response" (2014), at 1, available at http://www.enisa.europa.eu/media/press-releases/new-guide-by-enisa-actionable-information-for-security-incident-response (accessed 27 Nov 16).

Such observations form part of what is commonly known as incident response – identifying security problems, helping system owners and users remedy them, and using information to improve future security. Although the term "incident response" might suggest a purely reactive process, such activities should extend both before and after incidents occur. Early detection, perhaps even before a security vulnerability is exploited, can reduce the impact of current security problems; post-incident review can reduce the likelihood of future vulnerabilities and incidents.

Because incident response requires special skills, policies, processes and authorities, it is often assigned to a specific group within an organisation. Many different terms are used for these, including CSIRT (Computer Security Incident Response Team), CERT (Computer Emergency Response (or Readiness) Team) and IRT (Incident Response Team). This paper treats these as synonyms and uses the term CSIRT throughout. Each team has a defined constituency of people or organisations that are the main focus of its activities: for example, a region, country, sector, organisation, the purchasers of a particular product, or paying customers of the CSIRT itself. Different teams have different access to, and authority over, their constituency's systems: an organisational or commercial CSIRT may have direct control of its constituency's networks and computers; a National or Regional CSIRT may have no access to systems and be entirely dependent on others to provide data and to implement its advice.

The contribution of incident response to both privacy and data protection is increasingly recognised by legislators and regulators. Although the e-Privacy Directive (Recital 53)[8] and the Regulation (Recital 49) merely recognise incident prevention and response as "legitimate" activities, ENISA notes "[m]any EU documents have stressed the importance of [CSIRTs], especially their early warning and incident response capabilities".[9] Breach notification provisions in several European laws require organisations to assess, mitigate and notify any incidents affecting personal data.[10] The European Commission's Digital Agenda regards "a well-functioning network of [CSIRTs] … covering all of Europe" as a key support for "Internet trust and security … vital to a vibrant digital society".[11] Although Bruce Schneier considers that it has "taken industry a long time" to provide and use

---

[8] *Directive 2009/136/EC of the European Parliament and the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection or privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on c-operation between national authorities responsible for the enforcement of consumer protection laws*.

[9] ENISA, "Detect, Share, Protect" (2013), at 1, available at https://www.enisa.europa.eu/publications/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs (accessed 27 Nov 16).

[10] E.g. *Regulation (EU) 2016/679*, see note 4 above, arts 33-34; Directive 2009/136/EC Article 2(4)(c), *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*, art 19(2).

[11] Quoted in "Cybersecurity and the European Digital Agenda" (2015), available at https://www.cyberwiser.eu/content/cybersecurity-and-european-digital-agenda (accessed 27 Nov 2016).

"incident response products and services,"[12] Ruefle and colleagues note that "quicker containment … and earlier systems recovery" were identified as potential benefits as long ago as 1988.[13]

Most incident response can be divided into three stages: detecting security vulnerabilities, threats and incidents; notifying their (potential) victims; and sharing information to reduce the likelihood of them recurring. Different data, and different processing, are likely to be involved in each stage, so different legal issues may arise.

2.1 Detecting Problems

Many different information sources contribute to identifying security vulnerabilities, threats and incidents. For example, measurements of types and quantities of network traffic have been used for many years:[14] computers generating unusually large volumes of e-mail traffic may be being abused as distribution points for junk mail; users visiting websites known to be infected with malware may well infect other systems they use; devices looking up domain names associated with botnets are likely to be controlled by a malicious third party. Such indicators are found among huge volumes of data concerning routine, legitimate traffic. Some suspicious traffic patterns may be identified by equipment such as firewalls and intrusion detection systems. With attackers increasingly targeting applications and data, rather than the computers they run on, application logs will play an increasing role.

These sources are normally managed by the affected organisation, but they provide less than 40% of incident discoveries.[15] Other, less predictable, sources are also essential. Incidents may be reported by staff, customers, external parties (including other CSIRTs), or even by intruders themselves. Such reports contain highly variable amounts of information, from a single e-mail in which a virus was detected to the company's entire customer database.[16] Investigation often reveals additional information, either about that incident or others. Forensic analysis of compromised computers can produce very large collections of both relevant and irrelevant data.

Threats and incidents may also be discovered by retrospectively identifying patterns in log files. The first instances of new attacks are usually discovered from their impact on an individual victim account or computer. Subsequent investigation of these incidents often reveals a specific series of events or communications preceding the attack – a user visiting a particular website or receiving an e-mail from a specific sender, or a malicious program generating a particular sequence of packets in

---

[12] B Schneier, "The Future of Incident Response" (2014) September/October *IEEE Security and Privacy* 94-95.

[13] R Ruefle et al, "Computer Security Incident Response Team Development and Evolution" (2014) September/October *IEEE Security and Privacy* 16-26, at 19.

[14] ENISA, "Botnets: Detection, Measurement, Disinfection and Defence" (2011), at 42, available at https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence (accessed 27 Nov 16).

[15] HM Government, "Information Security Breaches Survey 2015" (2015), at 16, available at https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf (accessed 27 Nov 16).

[16] E.g. BBC, "Ashley Madison Infidelity Site's Customer Data Stolen" (2015), available at http://www.bbc.com/news/technology-33592594 (accessed 27 Nov 16).

establishing its communications links. Once these patterns are known, other victims can often be identified by checking for accounts or systems that display the same pattern. This technique may even identify compromised systems before they are exploited, thus protecting their users from the incident's most harmful consequences. However, the process of discovery, analysis and pattern identification takes time – ENISA note "it is not uncommon for certain persistent threats to be discovered, analysed and described months after initial compromise"[17] – while some detection patterns comprise a sequence of individually normal events. Retrospective incident detection therefore requires organisations to retain logs of apparently routine system and network activity. The development and sharing of detection patterns – known as Indicators of Compromise (IoCs) – will be discussed later.

2.2 Notifying Victims

When a security incident or vulnerability is discovered within its constituency, a CSIRT will usually wish to notify the owners and users of the affected systems. For teams without direct control of systems, this is the only way to contain incidents and mitigate their consequences. Owners need to restore their systems to a secure state; users may need to change passwords and assess the impact of any unauthorised access to information. The CSIRT may also want to work with owners to understand how the incident occurred, whether it has wider consequences, and how similar events might be prevented in future. Some teams may be able to contact owners and users directly, but more often (particularly for external CSIRTs) this will be done through a chain of trusted contacts within the affected organisation.

2.3 Sharing Information

As ENISA note, "[d]ue to the global nature of threats, it is common for a [CSIRT] to have information that is relevant beyond its immediate area of responsibility."[18] Vulnerabilities and incidents are rarely specific to a single organisation, so knowing how an attack was conducted and discovered can help others detect or prevent the same happening to them. Even more directly, since most attacks use compromised machines,[19] the external "attackers" in the CSIRT's incident logs are almost certainly themselves victims whose users also have serious privacy and security problems. When workload permits, most CSIRTs try to send specific warnings to victims outside their constituency, as well as sharing what they learned from the incident with their peers. Skierka and colleagues see this as "a positive-sum game, in which the security of one network will improve the security of the global Internet and vice versa."[20]

Much of the information that CSIRTs handle to reduce incidents and vulnerabilities could cause harm if misused. Application logs, in particular, may contain sensitive

---

[17] ENISA, "Actionable Information", see note 7 above, at 3.

[18] *Ibid*, 42.

[19] *Ibid*, 52.

[20] I Skierka et al, "CSIRT Basics for Policy Makers", at 21, available at http://www.gppi.net/publications/global-internet-politics/article/csirt-basics-for-policy-makers/ (accessed 27 Nov 16).

data; information about vulnerable systems can be used to compromise, as well as protect, them. Confidentiality is therefore both a routine practice and a fundamental norm in incident response work. Internally, CSIRTs need secure systems for reporting and collaboration: encrypted communications and closed mailing lists are commonly used.[21] Before notifying victims or sharing with others, unnecessary information, such as the identity of victims or data sources, is removed.[22] Wider sharing should be covered by a clear policy, and information marked, for example using the Traffic Light Protocol,[23] to indicate whether recipients may distribute it further.

Respecting such markings, and only using information in ways the sharer expects, are essential to participation in CSIRT networks. Recipients who do not "responsibly use, share, and protect information shared by others"[24] will quickly lose trust and be excluded from future sharing, thus damaging the community's ability to address security problems. Sharing information with law enforcement or other agencies who may use it for wider intelligence or offensive purposes can cause problems if these activities are perceived as conflicting with the expectation that CSIRTs' activities should improve overall security.[25] To maintain trust, such sharing may need to be done on a case-by-case basis, under the CSIRT's control and with the consent of the reporter or victim.

2.4 Incident Response in Future

As more data and services are provided on-line, incidents become more damaging to both individuals and society, so more important to prevent or mitigate. However, attacks are also becoming harder to detect. Ruefle and colleagues already find "attackers hid[ing] their … traffic in otherwise normal-looking protocols";[26] Bejtlich and colleagues expect at most a "slightly abnormal interaction" to reveal an attacker's presence.[27] Detecting these signs will require automated processing of a much greater quantity of data than CSIRTs currently use. For common, easily recognised attacks, automated mitigation, too, may be possible (as is already the case for most computer viruses). Although more data may pass through CSIRTs' detection systems, the vast majority relating to legitimate use will never be seen by a human.

Exchange of information between teams will also increase in importance. Analysing complex attacks already requires a range of data sources and technical skills beyond the capacity of any single CSIRT. Mitigating global attacks such as large-scale botnets requires international coordination. Prevention will be driven by higher-level information about attack methods, rather than today's addresses, domains and URLs

---

[21] ENISA, "Detect, Share, Protect", see note 9 above, at 5.

[22] ENISA, "Actionable Information", see note 7 above, at 46.

[23] Forum of Incident Response and Security Teams, "Traffic Light Protocol" (2016), available at https://www.first.org/tlp (accessed 27 Nov 16).

[24] R Ruefle et al, see note 13 above, at 19.

[25] I Skierka et al, see note above 20, at 20.

[26] R Ruefle et al, see note 13 above, at 22.

[27] R Bejtlich, J Steven and G Peterson, "Directions in Incident Detection and Response" (2011) January/February *IEEE Security and Privacy* 91-92, at 91.

that attackers can easily change.[28] Learning from others' experiences, and sharing your own, will be vital.[29] Recognising the need for "all actors in the cyber-security field … to share information on software flaws/vulnerabilities … security incidents and breaches" the European Data Protection Supervisor notes "[i]t is by acting together in a coordinated manner that we are most effective in ensuring cybersecurity for all."[30] Or, in ENISA's conclusion: "Local detection, accompanied by trusted forms of information exchange, leads to global prevention of cyber-attacks."[31]

3. Legal Analysis of Incident Response

European data protection law applies to:

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[32]

CSIRTs rarely need, or are able, to identify individual users.[33] Unlike law enforcement, their role is to defend their own systems, not to investigate or prosecute external attackers. Knowing that a particular Internet Protocol (IP) address behaves abnormally is usually sufficient. However, the European Court of Justice has recently ruled that so long as legal means exist whereby an organisation could identify the individual associated with an online identifier, information connected to that identifier must be treated as personal data irrespective of whether or not the organisation actually needs or intends to make that identification.[34] Furthermore, European law, unlike other jurisdictions', continues to regulate personal data that the individual has disclosed.[35] CSIRT processes should therefore handle information that may relate to a single subscriber or machine in accordance with data protection law. In performing incident detection and response, the CSIRT is likely to be determining the "purposes and means" of processing, so will be classed as a data controller, with specific legal responsibilities. In particular, the CSIRT must ensure that the processing is covered

---

[28] ENISA, "Actionable Information", see note 7 above, at 62.

[29] F Fransen, A Smulders and R Kerkdijk, "Cyber Security Information Exchange to Gain Insight into the Effects of Cyber Threats and Incidents" (2015) 132/2 *Elektrotechnik & Informationstechnik* 106-112, at 107.

[30] European Data Protection Supervisor, "Opinion 8/2015", see note 5 above.

[31] ENISA, "Detect, Share, Protect", see note 9, at iv.

[32] *Regulation (EU) 2016/679*, see note 4 above, art 4(1).

[33] K Silva and F Coudert, "ACDC – Legal Requirements" (2014), at 19, available at http://acdc-project.eu/wp-content/uploads/2015/05/ACDC_D1.8.1_Legal_Requirements.pdf (accessed 27 Nov 16).

[34] Case C-582/14, *Patrick Breyer v Bundesrepublik Deutschland*, at 49.

[35] J Kropf, "Google Spain SL v Agencia Española de Protección de Datos (AEPD). Case C-131/12" (2014) 108 *American Journal of International Law* 502-509, at 506.

by one of the grounds in Article 7 of the Data Protection Directive, now Article 6(1) of the Regulation.

The UK's Information Commissioner lists incident response processes – "containment and recovery; assessment of ongoing risk; notification of breach; evaluation and response"[36] – among the "appropriate technical and organisational measures to ensure a level of security appropriate to the risk" that data controllers may be required to implement to protect the security of personal data.[37] This appears to make the required processing of personal data "necessary to fulfil a legal duty," so lawful under clause (c) of Article 7. However, in other jurisdictions the relationship between incident response and data protection is much less clear. In some cases, essential processing may even be prohibited.

Breach notification requirements might justify some of the processing involved in the notification stage of incident response, but until the Regulation comes into force in May 2018, these only cover specific sectors, including network operators (under the e-Privacy Directive[38]) but not websites, databases or other networked computers. Furthermore, even under Article 33 of the Regulation, breach notification does not cover detection, which involves processing of data before a breach is discovered, nor the (potentially international) subsequent sharing of information with banks, Internet Service Providers (ISPs), software vendors and other organisations that may benefit from knowing how to prevent or detect vulnerabilities and incidents. Nor does it cover near-misses or security breaches that have not yet affected personal data, even though mitigating these and sharing information about them could help to prevent serious incidents elsewhere.

This section reviews the challenges and uncertainties that current legal systems create for incident response activities, and considers whether the Regulation could provide a common approach.

3.1 Diverse Approaches Under Existing Laws

Plohman and colleagues review the laws covering a common CSIRT task: the detection and investigation of botnets. These are groups of computers, hijacked without their owners' knowledge, used to attack other computers, networks and users. They find "national diversity" in definitions of cybercrime and a conflict between laws "whose aim is to ensure and ensure and improve overall internet security" and those on "user privacy and personal data protection."[39] They share Martin and Andrade's concern that, in some countries, data collection techniques "may not be

---

[36] Information Commissioner, "Guidance on Data Security Breach Management" (2012), at 2, available at https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf (accessed 6 Jul 16).

[37] *Regulation (EU) 2016/679*, see note 4 above, art 32(1).

[38] *Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)* (as amended by Directive 2009/136/EC), art 4(3).

[39] ENISA, "Botnets", see note 14 above, at 74.

unequivocally legal."[40] These authors raise two issues: how CSIRTs can collect necessary information in compliance with local law, and whether legal uncertainties and differing national interpretations may delay or prevent an effective response to incidents.

Vihul and colleagues compare Germany and Estonia – countries whose policies aim to encourage CSIRTs to monitor network activity and respond when computers join botnets. Yet "the seemingly harmless and routine technical action of inspecting packets and traffic is surrounded by a number of legal concerns."[41] German network operators can lawfully collect and analyse network traffic information, but only "to recognise, limit or eliminate a disturbance or error of their own telecommunications systems."[42] Monitoring for infections *before* an attack disrupts the network seems to be prohibited. Operators of networked services such as websites can only process personal data for the purpose of the service[43] (though, as discussed below, this restriction was challenged in 2016 by the European Court of Justice[44]). Estonian law permits processing unless individual users object. This is considered unlikely because "[t]he probability of the botmaster initiating any official proceedings is relatively low" and "the owner of an infected computer is not expected to turn against a researcher acting in good faith."[45] The authors conclude that "despite good intentions to mitigate or restrict the negative effects of botnets" legislation can "make it very difficult or impossible."[46]

Silva and Coudert agree that data protection law regulates botnet detection and remediation, but consider that it does permit the necessary data processing. The Advanced Cyber Defence Centre (ACDC) uses network sensors, website analysers, PC disinfection tools and a central clearinghouse to establish "an environment of data sharing and knowledge exchange among end-users, ISPs, [CSIRTs] and webmasters."[47] They argue that each component falls under a different clause of Article 7 of the Data Protection Directive.[48] Monitoring network and website traffic for signs of infection falls within Article 7(b) as necessary to fulfil the ISP's contract to provide its customers with a reliable and secure network service.[49] Alternatively, it could be covered by Article 7(c) as necessary for the public network operator's legal

---

[40] A Martin and N Andrade, "Battling Botnets with Digital Rights in Mind" (2012) 3(2) *European Journal for Law and Technology*, at 2.

[41] L Vihul et al, "Legal Implications of Countering Botnets" (2012), at 16, available at https://ccdcoe.org/multimedia/legal-implications-countering-botnets.html (accessed 27 Nov 16).

[42] *Ibid*, 23.

[43] *Ibid*, 31.

[44] Case C-582/14, see note 34 above.

[45] L Vihul et al, see note 41 above, at 27.

[46] *Ibid*, 48.

[47] K Silva and F Coudert, see note 33 above, at 9.

[48] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive)*.

[49] K Silva and F Coudert, see note 33 above, at 38.

duty, under Article 4(1) of the e-Privacy Directive, to ensure the security of its services. When customers run disinfection tools to remove botnets from their own computers, processing has the user's informed consent, under Article 7(a). Analysing and sharing information about the attack with other network and website operators is a legitimate interest of all parties, covered by Article 7(f), since it improves their ability to defend against similar threats. This sharing takes place through a clearinghouse which uses automation, data minimisation and access controls to minimise the potential impact on individuals whose data may be processed.

Silva and Coudert also consider whether incident response might be "a task carried out in the public interest," so justified under Article 7(e). However, data protection authorities "tend to limit the application of Article 7(e) to quasigovernmental activities only," so this approach would not fit a public-private partnership like ACDC.[50] Walden and Flanagan reach the same conclusion for honeypots – "vulnerable computer systems or networks designed to be attractive to hackers as a target for intrusion."[51] Honeypot logs contain information about intruder techniques, some of it personal data. They consider the grounds for this processing is Article 7(e) for law enforcement honeypots and Article 7(f) for those operated by others.

However, Robinson and Graux warn that using different grounds may create barriers to co-operation, because "[CSIRTs] may be more inclined to share information knowing that the peer operates under a legal framework affording the same protections to personal data."[52] A CSIRT applying the Article 7(f) balancing test to protect users' interests might well be reluctant to share information with a CSIRT using Article 7(e), which can override those interests. Similar problems may arise for recipients subject to law enforcement, freedom of information or breach notification requirements, since these may change the normal data protection safeguards or require information to be used for purposes other than incident response. National CSIRTs, in particular, should clearly state their legal position to reduce "the legal confusion aris[ing] from uncertainty about which legal framework concerning data protection would apply."[53]

Working across international borders – required in many incidents – involves even more legal barriers and uncertainty. Although Article 7(f) was designed to create a common European framework, and the Court of Justice has ruled against variations and additions that "undermine the value of the provision,"[54] a Commission study found only eight member states using the same wording for the balancing test, while four had added "extra obstacles" to the Article's use.[55] Before sending personal data outside the EEA, fifteen countries require "some degree of prior notification" to

---

[50] *Ibid*, 39.

[51] I Walden and A Flanagan, "Honeypots: A Sticky Legal Landscape?" (2003) 29 *Rutgers Computer & Technology Law Journal* 317-370, at 317.

[52] ENISA, "A Flair for Sharing – Encouraging Information Exchange Between CERTs" (2011), at 7, available at https://www.enisa.europa.eu/publications/legal-information-sharing-1 (accessed 27 Nov 16).

[53] *Ibid*, 68.

[54] K Silva and F Coudert, see note 33 above, at 72.

[55] *Ibid*, 7.

regulators.[56] Robinson and Graux conclude that "EU data protection regulations … may serve as a clear disincentive to the exchange of personal data by [CSIRTs] in international incidents that transcend the European context."[57] Silva and Coudert consider that sharing only non-personal data would have "very limited" benefits:[58] in particular, it would rule out warning victims of an attack, contrary to the Data Protection Directive's intention that individuals should be notified of processing (by intruders) of which they were not aware.[59]

It would, therefore, be possible to use different data protection grounds for different incident response activities and teams. Network providers might argue that improving network security was necessary to fulfil their contract with customers (Article 7(b)), or a legal duty under the e-Privacy Directive (Article 7(c)). Information about victims' own systems might be collected by consent (Article 7(a)). CSIRTs with national responsibility might act in the public interest or under official authority (Article 7(e)). However, as each ground has different safeguards, this would create significant difficulties in working together. Indeed, most teams already report legal uncertainties and national variations as barriers to effective cooperation.[60] Reducing these barriers requires a "more harmonised data protection regime that could apply to all [CSIRTs]."[61]

3.2 An Alternative Approach Under the General Data Protection Regulation

The Regulation, and the European Court of Justice's recent judgment in *Breyer*, suggest how such a common approach could be achieved. In *Breyer*, the Court ruled that website operators "may have a legitimate interest in ensuring … the continued function of those websites."[62] The operator must be allowed the possibility of using Article 7(f) of the Directive to cover necessary processing and German law's prohibition of this option (discussed above) was incompatible with the Directive.[63] Indeed securing networks, services and data should be a legitimate interest of most organisations, potentially covering all stages of incident response. Recital 49 of the Regulation explicitly supports the use of legitimate interests (now Article 6(1)(f)) for processing "strictly necessary and proportionate for the purposes of ensuring network and information security" by "public authorities, … CSIRTs, … providers of electronic communications networks and services and … providers of security technologies and services."[64] As a directly-applicable Regulation, this law should reduce the current inconsistencies between transpositions of the Directive.

---

[56] *Ibid*, 47.

[57] ENISA, "A Flair for Sharing", see note 52 above, at 30.

[58] K Silva and F Coudert, see note 33 above, at 48.

[59] *Directive 95/46/EC*, see note 48 above, arts 10, 11.

[60] ENISA, "A Flair for Sharing", see note 52 above, at 9.

[61] *Ibid*, 69.

[62] Case C-582/14, see note 34 above, at 60.

[63] *Ibid*, 63.

[64] *Regulation (EU) 2016/679*, see note 4 above, Recital 49.

However, Recital 49 does not guarantee full harmonisation. Recital 47 makes the contradictory statement that public authorities cannot rely on legitimate interests "in the performance of their tasks." The Article 29 Working Party note this must be interpreted to leave public authorities "some degree of flexibility":[65] in particular, the ability to participate in collaborative incident response. The *Breyer* judgment suggests how this might be done, noting that when operating websites, the Federal institutions "act, in spite of their status as public authorities, as individuals."[66]

The Regulation could also extend the same legal approach to international collaboration, by permitting transfers outside the EEA when "necessary for the purposes of compelling legitimate interests."[67] Article 49(1) covers exports that are "not repetitive, [and] concern[] only a limited number of data subjects": conditions that international incident response will normally satisfy. As under some implementations of the Directive, the requirement to inform Data Protection Authorities could introduce uncertainty.[68] However, Walden and Flanagan warn that "one can wait for legal clarity only at the expense of delayed or missed opportunity."[69] With the NIS Directive stressing that "cooperation between the public and private sector is essential"[70] and seeing global-scale security problems requiring "closer international cooperation to improve security standards and information exchange, and to promote a common global approach to security issues,"[71] these issues must be resolved without creating barriers between public and private, or EU and non-EU, CSIRTs.

As one of the widest grounds making processing lawful, legitimate interests is subject to the strongest safeguards. As following sections demonstrate, these safeguards are not only compatible with incident response work, in most cases they reflect good practice already adopted by the CSIRT community.

4. A Legitimate Interests Framework for Incident Response

The legal provision covering the widest range of incident response activities is therefore Article 6(1)(f) of the Regulation, which provides a legal basis for processing that:

> is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are

---

[65] Article 29 Working Party, "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" 844/14/EN WP 217, at 23.

[66] Case C-582/14, see note 34 above, at 53.

[67] *Regulation (EU) 2016/679*, see note 4 above, art 49(1).

[68] *Ibid*.

[69] I Walden and A Flanagan, see note 51 above, at 370.

[70] *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)*, Recital 35.

[71] *Ibid*, Recital 43.

> overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data[72]

The three-step test required by this Article – necessity, legitimacy and balancing interests – is a helpful guide to those planning and performing incident response; it provides additional safeguards, not required by other grounds for processing, for the individuals whose data they may process.[73] This section develops these requirements into guidelines for rights-protecting incident response. The next section applies these guidelines to specific activities involved in protecting computers, networks, users and information.

Recital 49 of the Regulation confirms that "ensuring network and information security", including "preventing unauthorised access … malicious code distribution … denial of service attacks and damage to computer and electronic communication systems," is a legitimate interest of CSIRTs. Processing personal data is a necessary part of this: Bradshaw notes that "[t]hreat-related information – such as Internet Protocol or email addresses – is essential" for CSIRTs to be able to counter phishing, malware and denial of service attacks;[74] Sylva and Coudert consider "securing networks without cooperation and information sharing is unfeasible."[75]

4.1 The Balancing Test

Despite the above commentary, the Article 29 Working Party's Opinion on Legitimate Interests notes that even processing that is necessary for a legitimate interest may be prohibited if it does not satisfy a balancing test:

> if the interest pursued by the controller is not compelling, the interests and rights of the data subject are more likely to override the legitimate - but less significant - interests of the controller. At the same time, this does not mean that less compelling interests of the controller cannot sometimes override the interests and rights of the data subjects: this typically happens when the impact of the processing on the data subjects is also less significant.[76]

The Working Party recommend assessing in turn the strength of the data controller's interest – which may "range from insignificant through somewhat important to compelling" – the impact on data subjects – which "may range from trivial to very serious," and any additional safeguards that can be provided.[77] The balancing test can then be applied to determine whether the processing may proceed.

---

[72] *Regulation (EU) 2016/679*, see note 4 above, art 6(1)(f).

[73] Article 29 Working Party, "Opinion 06/2014", see note 65 above, at 17.

[74] S Bradshaw, "Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity" (2015), at 11, available at https://www.cigionline.org/sites/default/files/gcig_no23web_0.pdf (accessed 3 Jun 16).

[75] K Silva and F Coudert, see note 33 above, at 56.

[76] Article 29 Working Party, "Opinion 06/2014", see note 65 above, at 26.

[77] *Ibid*, 30.

4.1.1 Data Controller Interest

Considering first the weight to be given to the data controller's interest, the Working Party consider this is greatest when the controller is exercising a fundamental right. Next are situations where the data controller's interest coincides with that of a wider community: "[s]ome interests may be compelling and beneficial to society at large,"[78] for example, "combatting financial fraud or other fraudulent use of services."[79] Other interests benefit the data controller alone. The Working Party identify "IT and network security" as an area where legitimate interests often arise.[80] Preventing, detecting and mitigating security incidents usually has benefits wider than the CSIRT or its parent organisation: it also benefits users of the affected systems (many of them also data subjects of the processing) by protecting the security of their information and activity; identifying botnets and software vulnerabilities may well have even wider benefits by protecting all Internet users from attacks that exploit these vulnerable systems.

In assessing its activities, a CSIRT should therefore consider both the severity of the incidents they are likely to prevent or mitigate and how widely those benefits can be shared. It may also consider the possible prejudice to those interests if it does not act.[81] Incidents that give an attacker control of computers are likely to have longer-term impact than those that make systems temporarily unavailable. Preventing attacks on others, or sharing information with victims or other operators to help them protect themselves, give the team's activities greater weight. Organisations should therefore plan such sharing as part of their incident response activities.

An interest carries more weight if it is "clearly acknowledged and expected … in the community and by data subjects that the controller can take action and process data in pursuit of these interests."[82] The growing recognition that networks and information systems must be protected (thus also protecting the rights of their users) and of the role of incident response should mean such activities are indeed "acknowledged and expected." Laws, such as the Regulation, that "specifically allow" such activities also contribute to these expectations.

4.1.2 Data Subject Interest

The other side of the balancing test assesses the impact of the processing on data subjects. The Working Party suggest as relevant factors the nature of the data involved, how they are processed, the reasonable expectations of the data subject, and the relationship between the data subject and the data controller.[83]

As discussed earlier, most of the data CSIRTs handle is associated with identifiers that the team cannot link to an individual user, for example IP addresses allocated by other networks. There should be no need to identify or distinguish individuals unless

---

[78] *Ibid*, 24.

[79] *Ibid*, 35.

[80] *Ibid*, 24.

[81] *Ibid*, 55.

[82] *Ibid*, 35.

[83] *Ibid*, 38-40.

they are involved in an incident, so the risk of this processing for most users is very low. Where a victim of an incident does need to be identified, the positive impact of notifying them may be taken into account,[84] so the net impact should still be low or, indeed, positive. Processing local identifiers, where linking information may exist within the same organisation, may involve a slightly higher risk. There may also be concern because of existing relationships between the organisation and the individual, for example as an employee or student. CSIRTs handling such information should be particularly careful to apply "functional separation" to ensure it is only used for network and information security.[85] Some CSIRT activities do not require processing personal identifiers at all, for example analysing malicious software or sharing details of a software vulnerability with other teams. Here inappropriate disclosure presents a higher risk to technical security than to personal data, so CSIRTs' normal practices for handling this type of material are likely to be ample for data protection purposes.

The balancing test will be harder to satisfy if the impact of processing is uncertain.[86] Where a CSIRT collects data from its own systems, or receives structured data from others, it can design the collection processes to extract specific information, such as packet headers or email addresses. Here the likely privacy impacts can be predicted and processes designed to minimise them. In other investigations, for example when a CSIRT is given a compromised computer or networked service to investigate, it is not possible to predict what kinds of personal information it may contain. Such investigations require particular care, and should use technical and organisational safeguards appropriate to this uncertainty. The need for a stronger interest to justify processing may mean the acceptable uses of unstructured data are more limited.

Although the CSIRT's interest in processing will be strengthened if it can share the resulting security benefit with others, this must be balanced against the increased impact if sharing involves wider dissemination and storage of personal data. The quantity of personal data that needs to be shared to mitigate or prevent an incident will generally be very small. The most obvious benefit of sharing information is to notify someone whose computer or account appears to have been compromised. Since the information processed by CSIRTs will not normally enable them to identify or contact the individual directly, notifications are usually sent to the individual's own organisation or ISP, who can identify and contact them. Similarly, for an account name or credit card number, the CSIRT may notify the relevant on-line service or bank. Since such recipients have an obvious interest in protecting the information and ensuring the problem is fixed, the balance between benefit and impact will normally be maintained. Where CSIRTs discover information about threats, vulnerabilities or defences, sharing these can also improve wider security. This is normally done within information sharing communities that have agreements on how information will be protected and used, keeping the risk at a low level.[87] CSIRTs should nonetheless

---

[84] *Ibid*, 37.

[85] *Ibid*, 51.

[86] *Ibid*, 40.

[87] E.g. CPNI Information Exchanges, available at http://www.cpni.gov.uk/about/Who-we-work-with/Information-exchanges/; European FI-ISAC, available at https://www.enisa.europa.eu/topics/cross-cooperation-for-csirts/finance/european-fi-isac-a-public-private-partnership; Trusted Introducer, available at https://www.trusted-introducer.org/services/overview.html; FIRST, available at https://www.first.org/.

consider whether the desired security benefit can be achieved without sharing personal information; if not, sharing is likely to be justified only when required to mitigate a clear and serious threat.

4.1.3 Additional Safeguards

Finally, the Working Party note that additional safeguards that reduce the risk of harm to data subjects "may in some cases play a role in tipping the balance in favour of the controller."[88] The Working Party mention encryption (in both storage and transmission) and pseudonymisation, both of which are already standard operational practice among incident responders. Indeed, most of the personal data processed by CSIRTs will already fall within the Regulation's definition of pseudonyms.[89]

The Working Party's earlier Opinion on Privacy Issues Related to the Provision of Email Screening suggests that a recent development in incident response practice – automated screening of alerts to reduce the number escalated to human incident responders – may function as an additional safeguard. The Working Party concluded that automated scanning of all e-mails to detect viruses might be acceptable provided the content was "kept secret and must not be disclosed to anyone but the addressee."[90] This treats inspection by computer as less of a privacy risk than inspection by human. Processes that reduce the need for human inspection of personal data, by limiting this only to alerts or sequences that exceed a designated threshold, should therefore be regarded as supporting the CSIRT's legitimate interest.

4.2 Summary

The requirements of the Article 6(1)(f) balancing test appear very similar to existing incident response good practice. This should not be surprising. CSIRTs are already aware that misuse of the information they handle could damage the security of networks, systems and data. The measures taken to prevent security harms also contribute significantly to data protection and privacy.

The analysis here indicates that a rights-focussed assessment should consider, when assessing the CSIRT's legitimate interest:

- The potential or actual severity of the incident being prevented, detected or investigated;
- How widely the CSIRT's activities will benefit others;
- Whether the objectives and activities fall within the reasonable expectations of those whose data will be processed, for example whether they are recognised as legitimate by the law or community norms;

And when assessing the impact on data subject rights:

- Whether the activity involves processing identifiers that might be linked to individuals, and how likely such linkage is;

---

[88] Article 29 Working Party, "Opinion 06/2014", see note 65 above, at 41.

[89] *Regulation (EU) 2016/679*, see note 4 above, art 4(5).

[90] Article 29 Working Party, "Opinion 2/2006 on privacy issues related to the provision of email screening services" 00451/06/EN WP 118, at 6.

- How the processing can be separated from other functions of the organisation;
- Whether information was collected in a way that included privacy safeguards;
- How widely information will be disclosed, and the interests of all recipients;
- What safeguards – including pseudonymisation, encryption and computer, rather than human, inspection – can be used.

The CSIRT can then use the balancing test to decide whether or not to proceed with the activity. According to the Working Party:

> Legitimate interests of the controller, when minor and not very compelling may, in general, only override the interests and rights of data subjects in cases where the impact on these rights and interests are even more trivial. On the other hand, important and compelling legitimate interests may in some cases and subject to safeguards and measures justify even significant intrusion into privacy or other significant impact on the interests or rights of the data subjects.[91]

Section 5 applies this test to typical incident response activities.

5. Applying the Framework to Incident Response in Practice

Three different stages of incident response may involve processing personal data: gathering and analysing data to identify and investigate vulnerabilities, attacks and incidents; informing and assisting victims; and sharing information to help others improve the security of their systems and networks. This section applies the legitimate interests balancing test to practical examples of each of these.

5.1 Detecting Security Problems

5.1.1 Network logging

A fundamental information source for those protecting networked computers is the patterns of communication between them: which machines communicate with which others, using which services.[92] Unusual patterns often indicate problems. For example, external computers normally communicate with few advertised servers – web, e-mail etc. – so attempts to contact PCs, webcams or other endpoints often indicate a scan for vulnerabilities. Internal systems should send email through a central hub, so direct connections to external addresses suggest a compromised system is being used to send spam. Connections between machines may be logged by routers, usually in the form of flows ("between times M and N, address A sent X packets/Y bytes to address B on port P"). Firewalls may generate alerts when unexpected connection attempts are made, for example accesses to an intranet server from offsite. Since attacks and incidents will often be detected from a sequence of these events,[93] such logs need to be retained, ideally for a period of weeks or months.

---

[91] Article 29 Working Party, "Opinion 06/2014", see note 65 above, at 30.

[92] ENISA, "Actionable Information", see note 7 above, at 6.

[93] E.g. D Raywood, "Swiss Attack Conducted by Patient and Sophisticated Hackers" (2016), available at http://www.infosecurity-magazine.com/news/swiss-attack-patient-and/ (accessed 27 Nov 16).

Historic logs can extend the benefits of incident detection from one machine to many: when one compromised machine is discovered, logs can be checked for others showing the same pattern of activity that may well have suffered the same fate.

The balancing test can be applied to the recording and processing of flows and alerts. Compromised computers represent a threat to the privacy and security of their users, their organisations and, in many cases, others connected to the Internet. Depending on the computer's function, the consequences could range from exposing all data it holds to risks to life in medical and industrial control environments. Without logs these incidents will be hard to detect and impossible to investigate. The legitimacy of an organisation processing personal data for these purposes is recognised by European law; it should be expected by Internet users.

Some of the logged IP addresses will constitute personal data under EU law (for most legitimate connections at least one of the endpoints will be a server, whose address does not relate to any individual). A CSIRT is very unlikely to need, or be able, to link external addresses to individual users: this would be done by a law enforcement agency, using its powers to obtain customer records from ISPs as part of a criminal investigation. For internal addresses there is no need to identify or single out machines or users that show normal activity. When abnormal activity is detected, users are identified and contacted as one of the last stages of the investigation, once harmless explanations have been eliminated and there is strong evidence that a security breach has in fact occurred. Identification of users is often done by a different team. Thus most personal data handled by the CSIRT will be pseudonyms, with information permitting linkage to data subjects kept separate and protected by technical and organisational measures.[94] Network-layer information is structured (e.g. the header fields of a TCP/IP packet), so systems and processes can be designed to apply appropriate privacy protections to each field. Information not relevant to incident response can be excluded. Preliminary analysis is increasingly computerised, with human incident responders only alerted when automated checks identify a significant likelihood of an incident. In many organisations, most log entries will never be seen by a human. Finally, organisations have a strong incentive to keep logs and other incident response records secure and confidential, as they contain information about compromised and vulnerable systems that could harm the organisation if disclosed or misused.

These factors suggest that logging flow data and alerts presents a very low risk to individual users. Investigating particular incidents may represent a slightly higher risk, but occurs when both the organisation's and the individual's interest in having the problem resolved are also increased. In each case the existing and developing practice of incident response should easily satisfy the balancing test.

5.1.2 Application logging

There may be a higher risk of intrusion when incident response uses logs at the application level. For example, a list of domain names requested could reveal more about the particular information that a user was seeking. Domain names cover a wider range of sensitivities than IP addresses: knowing a user has accessed *www.dignitas.ch* is more intrusive than *www.bbc.co.uk*, but both facts will appear in the same log file.

---

[94] *Regulation (EU) 2016/679*, see note 4 above, art 4(5).

However, application-level logs are critical to incident detection and investigation. For example, many botnets reveal themselves by the non-existent domains they query while attempting to contact their controllers.[95] Query logs identify these botnets before they do damage, whereas network flow data will only find them after malicious activity has occurred. Incident response processes must therefore ensure the balancing test is still satisfied.

With application-level data, it is particularly important to separate processes investigating security incidents from those investigating breaches of other organisational policies. Security incidents create different harms for both the organisation and individuals, so the balancing test is different. Furthermore, technical investigations aim to secure computers, so can use privacy protections (such as pseudonymisation) that are not available when investigating a particular individual's misbehaviour. The greater sensitivity of application data may mean it should be examined only after an increased risk has been identified from network traffic data or other sources. For example, DNS resolver logs can be searched for signs after a particular malware family has been characterised and its indicators of compromise determined. Alternatively, it may be possible to carry out at least the initial stages of investigations using anonymised data.

A particularly interesting technique is "passive DNS".[96] This discards all information linking a query to a particular user or machine, recording only the time and the response returned from public DNS information at that moment. Requests for local DNS information are usually excluded. Many malicious activities create characteristic patterns: domains that frequently change location or show sudden changes in popularity often indicate botnet controllers or phishing campaigns. CSIRTs can identify and validate these external threats from passive DNS logs, then search their traffic or application logs for local machines that have communicated with them. Compromises of local systems and accounts can be identified quickly using very specific searches, without processing any personal data of those not affected.

Since passive DNS discards local identifiers, the risk to local users is extremely low.[97] All information is obtained from public sources. Most will relate to servers, so is not personal data. Even where it does relate to a single-user computer, processing information from a public directory should not be unexpected and represents a minimal increase in privacy risk. If required, logging systems can be tuned to record only DNS record types whose value for detecting threats exceeds their privacy impact. As will be discussed below, passive DNS data can be shared, increasing their value and, through aggregation, providing even better privacy protection.

5.1.3 Pastebin dumps

A common way to discover successful attacks is from information published by attackers themselves. Lists of compromised accounts and systems are often placed on

---

[95] E.g. Y Zhou, Q Li, Q Miao, K Yim, "DGA-Based Botnet Detection Using DNS Traffic" (2013) 3 *Journal of Internet Services and Information Security* 116-123.

[96] F Weimer, "Passive DNS Replication" (2005), available at http://www.enyo.de/fw/software/dnslogger/first2005-paper.pdf (accessed 27 Nov 2016).

[97] M Keio, "Privacy Considerations for ISC Passive DNS" (2012), available at https://archive.farsightsecurity.com/Passive-DNS-Privacy.pdf (accessed 27 Nov 2016).

public forums, either to demonstrate the attacker's prowess, to invite offers to buy larger collections of information, or to seek assistance in cracking encrypted passwords. Many CSIRTs monitor such forums for mentions of their own organisations or constituencies in connection with security problems.[98] When a relevant post is discovered, it will normally be downloaded for further analysis. Although this information may be unreliable – intruders are rarely precise about their source and sometimes publish out of date information – it can indicate when and where additional checks are required. Even a partial list of compromised accounts can help find others by checking for similar patterns of activity in the organisation's own logs.

By publishing information about insecure systems or compromised accounts, the attackers have already harmed the security and privacy of those systems and users. The CSIRT's actions, by ensuring prompt action is taken to remedy the insecurity, should limit further intrusion and minimise the harm done by the publication. Since teams cannot control what information may be found on a forum, their processes should be designed to minimise any additional risk to security and privacy. In particular, information should only be gathered where remedial action is likely – typically information about the team's own constituency. For practical reasons, most searches are conducted automatically by programs that ignore irrelevant information; results for human analysis should be held securely and only for as long as necessary.

Despite the difficulty of predicting what information will be encountered on forums, these safeguards should be sufficient to satisfy the balancing test and justify the processing. The justification may be further strengthened by informing users of compromised systems or accounts – thus increasing the number who benefit from the processing – as described in the next section.

5.2 Notifying Victims

5.2.1 Direct contact

A CSIRT will often obtain information, either from its own monitoring systems or by a notification from another team, indicating a security problem with a computer or user account within its constituency. A computer may connect to a known malware control server, or a sudden increase in logins to a webmail server suggest that a user's password has been phished and is now being used to send spam. Most teams would wish to inform the user of the problem and help them to fix it: this removes a threat to the user's privacy and data protection rights and – since compromised accounts and systems are one of the main routes to attack systems, networks and data – a direct threat to the organisation's interests as well. Two steps, both involving processing personal data, are involved: determining from local logs which user or subscriber account is associated with the activity, and using stored contact details to inform them of the problem.

---

[98] L Harrigan, "Using Data from Pastebin.com for Incident Response and Investigation" (2012), available at https://webmedia.company.ja.net/content/presentations/shared/csirt051112/harrigan/slides.pdf (accessed 27 Nov 16).

Applying the balancing test, a compromised account or computer severely impacts the privacy and data protection rights of its users, by letting the attacker read or modify any information the legitimate user can, or perform any action under their identity. A CSIRT has a strong interest in helping members of its constituency avoid such harm, and also in preventing their systems being used as a launch pad to attack others. Informing users of security problems is encouraged by law and community norms, so should be expected by those users. Users cannot be contacted – whether by e-mail, letter or in person – without processing directly identifying information collected when their account was created. However, that information need only be disclosed to the affected individual, who will receive the greatest benefit from the processing. Teams handling large numbers of notifications may use automated systems to identify and contact the relevant subscribers.

Balancing interests and harm, the user is likely to suffer far worse harm if they continue to use a compromised system, unaware of the problem, than from the very limited personal data processing required to inform and assist them.

5.2.2 Brokerage

Some constituencies are sufficiently large that separate CSIRTs exist within them. This often applies, for example, to national-scale teams. Rather than every team doing its own information gathering, trusted teams may act as brokers obtaining information about their whole constituency and passing on relevant sections to other teams. This might include incident information from forums or notification services, lists of compromised accounts discovered during forensic analysis, or warnings of vulnerable systems from vendors and security researchers.[99] For example, many National Research and Education Network CSIRTs receive information concerning their customer universities and colleges and redistribute portions to the relevant site contacts. While researchers, services and broker CSIRTs may have little direct interest in information that does not relate to their own systems, by distributing that information through trusted and secure channels, they can facilitate a quicker and more privacy-protecting response. As one example, when a researcher discovered nearly six million Internet hosts whose communications could be decrypted by the DROWN attack,[100] individual warnings to more than half of them were distributed securely through the global CSIRT network.[101]

The balancing test suggests that facilitating the transmission of information about security vulnerabilities and incidents to those able to resolve them can be a legitimate interest. Since laws increasingly expect breaches to be reported, it should fall within the reasonable expectations of Internet users. To minimise the impact on individuals' rights, researchers and brokers should ensure information is passed securely to individuals or organisations that can be trusted to use it appropriately. CSIRTs performing this role normally have lists of such contacts and established ways to

---

[99] ENISA, "Detect, Share, Protect", see note 9 above, at 25.

[100] N Aviram et al, "DROWN: Breaking TLS using SSLv2" (2016) *Proceedings of the 25th USENIX Security Symposium*, available at https://drownattack.com/drown-attack-paper.pdf (accessed 27 Nov 16)

[101] Personal communication with Dr Klaus-Peter Kossakowski, PRESECURE Consulting GmbH (1 Mar 16).

communicate with them. Information should only be sent if it is likely to be acted on: brokers should ensure their processes for allocating information to recipients are accurate, and may check in advance that recipients are able to use it. If not, there is no point incurring even a very small risk to individuals' interests.

A well-planned brokerage activity will protect individual rights better than either having those who discover security problems send all information to everyone who might be interested, or having them give up and not notify anyone because the challenge of secure distribution is too hard.

5.3 Sharing Information

Incident response activities create the greatest benefit when knowledge is shared, letting other organisations detect or prevent similar incidents on their own networks. Sharing could also represent the greatest risk to privacy and data protection rights, so the balancing test's guidance on when and how to share is especially relevant. Sharing among the CSIRT community has always aimed to reduce, rather than increase, security risks: the resulting practices already provide good protection for individual rights as well.

Some types of knowledge sharing involve no personal data. Passive DNS data was discussed above as a way organisations can identify external threats without processing information about individual users. Contributing this data to shared repositories provides further benefits by revealing wider patterns such as domains that resolve differently depending on the location or timing of the request.[102] By aggregating multiple sources, repositories further reduce the risk of any query being associated with a particular user. Contributing organisations may withhold any record types or queries that they consider involve an excessive risk.

Warnings derived from passive DNS data are one example of an Indicator of Compromise (IoC). These are patterns that organisations can search for in their own records or systems that are likely to indicate an incident. Simple examples might include "file called xyz123 suggests malware present on a PC," "traffic sent to port X on IP address Y may indicate a remote access tool," or "e-mail from user A@B probably a phishing attempt." More complex IoCs include file hashes,[103] patterns of system calls,[104] and information on attacker campaigns.[105] Attackers continually develop new attacks, so security teams and technologies from anti-virus to firewalls rely on up-to-date supplies of IoCs to detect and prevent them. As the examples illustrate, IoCs may contain personal data so must be shared in ways that protect rights.

While only a few teams have the specialist skills and data sources to create and provide IoCs as a community or commercial service, most CSIRTs develop them while investigating and detecting incidents on the networks and systems for which

---

[102] Farsight Security, "DNSDB" (2016), available at https://www.farsightsecurity.com/solutions/dnsdb/ (accessed 27 Nov 2016).

[103] ENISA, "Detect, Share, Protect", see note 9 above, at 13.

[104] ENISA, "Actionable Information", see note 7 above, at 7.

[105] F Fransen, A Smulders and R Kerkdijk, see note 29 above, at 107.

they are responsible. When compromised computers are found, teams will normally try to identify signs they can use to check whether other systems have experienced the same attack. Sharing IoCs with other teams can improve security more widely, but may also involve data protection, privacy and security risks. The balancing test can help CSIRTs decide whether or not to do so.

Indicators of compromise, as their name suggests, relate to incidents that harm individual rights. Helping others prevent or reduce the impact of such incidents clearly has a benefit. This is greater for incidents likely to affect many systems and individuals. The incident's impact is also relevant: an incident that lets an attacker control a computer places the privacy and security of all its users and data at risk. An IoC to detect a new attack or incident has greater benefit than one that is already known and detectable. Sharing information about incidents, to help others avoid them, has been part of the CSIRT role since the concept was invented and is increasingly recognised and even required by law.[106]

Such sharing rarely requires disclosure of information about local users, who are the most likely to be identified, either deliberately or accidentally. However, some IoCs must include information that may relate to an external individual – for example, the text of a phishing e-mail, the email or IP address from which an attack came. It will rarely be possible to anonymise these IoCs without making them useless for preventing or detecting local instances of the same incident. However, preventing and detecting incidents does not require linking these identifiers to the individual (if any) associated with them. Identification is only necessary when a CSIRT wants to inform a victim that their account or computer has been compromised (discussed under Notification above) or where law enforcement wishes to pursue the actual attacker. These distinct purposes should be clearly separated and the appropriate legal provisions applied.

IoCs are normally shared either within trusted communities with their own agreements on reuse,[107] or with companies or clearinghouses applying their own non-disclosure and sanitisation processes.[108] Wider sharing is only likely in the most serious incidents, where the risk of helping attackers is outweighed by the impact if the security problem is not addressed. Impacts on rights can be reduced by sharing IoCs in a structured, machine-readable format. A CSIRT that can consume and use IoCs automatically, as is routinely done for example with virus signatures, need never see the actual IoC and any potential personal data it may contain.

The balancing test can guide CSIRTs when an incident may be sufficiently minor and require too much personal data for sharing to be justified. It can also help identify the most serious incidents where global sharing is appropriate. But for most incidents, the practices already followed by CSIRTs to protect sensitive information should be sufficient to allow sharing within their trust networks.

---

[106] e.g. *NIS Directive* (EU) 2016/1148, art 14(3).

[107] R Ruefle et al, see note 13 above, at 20.

[108] E.g. Circl.lu, "Malware Information Sharing Platform (MISP)" (2016), available at https://www.circl.lu/services/misp-malware-information-sharing-platform/ (accessed 27 Nov 16).

6. Conclusion

For both privacy and data protection, the security of networks, computers and information is vital. However incident response – detecting security vulnerabilities and incidents, mitigating their impact and improving future security – requires the processing of personal data. Past legislation and interpretation has resulted in an unclear and inconsistent regulatory environment: sometimes preventing incident response, more often creating uncertainties that discourage collaboration in particular. Cross-sector and international coordination, essential when all Internet security problems are potentially global in scope, are particularly badly affected.

In contrast, Recital 49 of the new Regulation offers a clear, consistent and comprehensive legal framework, declaring incident response a legitimate interest of organisations. This ground for processing requires the strongest safeguards: processing may not take place unless the benefits clearly outweigh any risks. However these data protection requirements are very similar to CSIRTs' existing need to protect security-sensitive information. Current incident response practice largely satisfies the conditions required for processing under legitimate interests.

This article has derived a legal framework for incident response from the Regulation, and has shown how CSIRTs can apply it to their activities. In the future, this should reassure CSIRTs and Internet users that incident response is both supported and encouraged by European data protection law, considered the strongest in the world. Perceived and actual legal barriers should no longer stop us protecting Internet users, their computers and data.