The shape of things to come: the Equifax breach, the GDPR and open-source security


Daniel Hedley


Matthew Jacobs

Daniel Hedley, Irwin Mitchell LLP and Matthew Jacobs, Black Duck Software

Although the General Data Protection Regulation (GDPR) is being hailed as a sort of revolution, what it really represents is the law catching up with reality. The GDPR isn't alone, of course – in the information security space it is accompanied by the Network and Information Security Directive (NISD). Both the GDPR and NISD go into effect in May 2018.

The GDPR deals with a lot of things beside information security, covering a wide range of topics, from people's rights of access to their data to automated decision making, from the treatment of biometric data to the rules on appointing a data protection officer. Of particular note in the infosec space is article 32, which requires organisations subject to the GDPR to take "appropriate technical and organisational measures to ensure a level of security appropriate to the risks" to the "rights and freedoms of natural persons" which arise out of those activities. The appropriate level of security is to be assessed by reference to three things:

- The likelihood and severity of the risk.
- The 'state of the art' (that is, measures that are available).
- The cost of implementation.

Of itself, that three-way balancing act is not new and closely corresponds to current EU law. However, the GDPR makes two important changes.

The first and most important change is that this obligation applies to data controllers and data processors alike. Under the current regime, the data processor has no direct obligations to the regulator or to the data subject (ie, people). Its obligation is to the data controller and subject to whatever limitation on its liability it has managed to negotiate into that contract. Under the GDPR, the data processor – typically the vendor/supplier in the technology world – has direct liability and accountability for security breaches, both to the regulator and to those affected.

The second change is to the scope of organisations caught by the GDPR: unlike the old law, which focused on businesses with establishments or hosting arrangements within the EU, the GDPR can (in some circumstances) affect organisations with no physical EU presence at all.

Common challenges

In a breach disclosure notice made in early September, US-based credit reference agency Equifax said criminal hackers had exposed the personal data of 143 million customers in the US (later revised upwards to over 145 million), which was stolen between mid-May and late July this year after taking advantage of a "web application vulnerability". Equifax also holds the personal details of 44 million UK citizens, according to reports, and admitted without going into details that "limited personal information" from British and Canadian residents had also been compromised.

Equifax issued a statement on September 13 acknowledging that the breach was due to a vulnerability in Apache Struts, a free, open-source framework for creating web applications that is widely used by Fortune 100 companies to build corporate websites. Organisations such as Lockheed Martin, the IRS, Citigroup, Vodafone, Virgin Atlantic, Reader's Digest, Office Depot and ShowTime have all developed applications using the Struts framework.

"According to the ICO's published penalty notice, the Gloucester Council breach was relatively small-scale, with compromised personal data relating to around 30-40 people. Nevertheless, the ICO considered a monetary penalty to be appropriate"

That vulnerability was CVE-2017-5638, which was reported in March of this year. That Struts flaw allows an attacker to execute requests to an Apache web server and provides an easy way to take control of sensitive sites.

Would a failure to secure against a vulnerability, disclosed and patched months before, breach Article 32 of the GDPR if personal data was stolen using a hack exploiting that vulnerability?

The perennial 'lawyer's answer' is 'it depends', but a UK case from earlier this year provides an instructive example of how it could.

"No less than 83% of audited applications in the retail and e-commerce industries contained high-risk known open-source vulnerabilities"

The UK data protection regulator, the Information Commissioner's Office (ICO), recently fined Gloucester City Council following an attack that led to a compromise of internal emails.[1] According to the ICO's published penalty notice, the Gloucester Council breach was relatively small-scale, with compromised personal data relating to around 30-40 people. Nevertheless, the ICO considered a monetary penalty to be appropriate. The reason given by the ICO in that case was that the vulnerability exploited by the attacker was the well-publicised 'Heartbleed' vulnerability in OpenSSL, among the most common open-source components used by organisations.

The common thread connecting the Equifax and Gloucester City Council cases is that the attacks were made possible by known but unpatched vulnerabilities in open source components. When you think about it, that's unsurprising. Open source is ubiquitous in today's applications because using open source lowers development costs, enables innovation and speeds time to market. Last year, Black Duck's Centre for Open Source Research & Innovation (COSRI) analysed more than 1,000 applications that were audited as part of M&A transactions. The COSRI audit analysis found that 96% of the applications scanned contained open source software.[2] But more tellingly, more than 60% of those applications contained known (but un-remediated) open source security vulnerabilities.

Notably, 60% of the financial industry applications that were audited contained high-risk open vulnerabilities. Additionally, the COSRI analysis showed that no less than 83% of audited applications in the retail and e-commerce industries contained high-risk known open-source vulnerabilities. On average, the open source vulnerabilities identified in the audited applications had been publicly known for more than four years.

Knowing your code

It's important to differentiate between open source components and open source vulnerabilities when talking about the need for open-source security. Open source is no less secure than proprietary/commercial code. Nearly all open source vulnerabilities are patched soon after the vulnerability is disclosed. But unlike commercial software – Microsoft's for example – critical open source security updates are not pushed to users as they become available. It's up to open source users to know what open source they are using and to stay on top of the various patches, fixes and upgrades made to their open source packages. As the COSRI audit analysis shows, many companies are not at all effective in doing this.

"All of the larger fines issued by the ICO have been for security breaches – for example, the TalkTalk and Playstation Network cases. Other European regulators are also known to take a harder-line view"

The issue is that too many companies lack visibility into and control over the open source they are using. Many organisations don't pay sufficient attention to the additional security exposures created by vulnerable open source components and actually may not even be aware these exposures exist in their applications or websites.

Returning to the law, a lot has been made of the greatly increased maximum fining powers in the GDPR (for the most serious breaches, up to €20m or 4% of global turnover, whichever is the higher), and it is perhaps a little trite to shout about the potential for massive fines and leave it at that. The ICO, at least, has made it clear that it has no intention of imposing huge fines for less serious breaches and that it views its fining powers as a last resort.[3] Nevertheless, it considered the much smaller Gloucester City breach to merit a fine of 20% of the current maximum and (to the best of our knowledge) all of the larger fines issued by the ICO have been for security breaches – for example, the TalkTalk and Playstation Network cases. Other European regulators are also known to take a harder-line view.

Consider something on the scale of the Equifax breach. If that were to happen under the GDPR regime, the consequences for the organisation concerned would be likely to be very serious indeed. Quite apart from the regulators' intervention and fining powers, the resulting litigation and reputational damage could run for years.

Protecting yourself

The most effective way for companies to get visibility into and control over open source in their applications and websites is to use automated processes to scan for open source, create an inventory of those open-source components and then map that open source to open source vulnerability databases. This enables them to identify any known vulnerabilities and then monitor their open source component inventory for any newly reported open source vulnerabilities.

With this visibility and vigilance, organisations can effectively protect themselves and their customers from the type of open-source exploit that affected Gloucester City Council and Equifax. They can avoid the fire drill that is going on right now at many large corporations that are trying to determine if they will be the next to be exploited by some vulnerability and be placed in a very uncomfortable media spotlight.

Although an organisation's compliance with GDPR will be self-assessed, you

will need be able to explain how you've addressed data privacy protection and justify your decisions if a data breach occurs after the regulations go into effect. Use of open source is not a special case, ignorance of your use of open source will be a weak defence and you need to manage vulnerabilities in open source just as you would any other software you use.

The consequences for inaction can be serious, both for you and for your customers, so our advice is to get processes and policies into place immediately to identify, manage and secure the open source used in your applications and web properties. As Benjamin Franklin once said: "An ounce of prevention is worth a pound of cure."

About the authors

Dan Hedley is a partner at law firm Irwin Mitchell LLP. He advises businesses on software licensing and development, IT service contracts, outsourcing and cloud services. He also advises on open source compliance, data protection, software IP issues and the IT aspects of M&A and IPO transactions. He regularly acts for both established corporates and early-stage and fast-growth businesses.

Matt Jacobs is vice-president and general counsel at Black Duck Software. He oversees the worldwide legal affairs of Black Duck including managing licensing and contract negotiation, managing the company's intellectual property portfolio and advising senior management on day-to-day legal affairs.

References

1. 'Supervisory Powers of the Information Commissioner: Monetary Penalty Notice'. Information Commissioner's Office, 26 May 2017. Accessed Oct 2017. https://ico.org.uk/media/action-weve-taken/mpns/2014217/gloucester-city-council-mpn-20170525.pdfhttps://ico.org.uk/media/action-weve-taken/mpns/2014217/gloucester-city-council-mpn-20170525.pdf.
2. 'Black Duck's 2017 open source security and risk analysis finds security and compliance risks in most applications'. Black Duck. Accessed Oct 2017. www.blackducksoftware.com/open-source-security-risk-analysis-2017.
3. 'GDPR – sorting the fact from the fiction'. Information Commissioner's Office blog, 9 Aug 2017. Accessed Oct 2017. https://iconewsblog.org.uk/2017/08/09/gdpr-sorting-the-fact-from-the-fiction/.

Hobby hackers to billion-dollar industry: the evolution of ransomware


Srinivasan CR

Srinivasan CR, Tata Communications

In recent months, ransomware has become a mainstream topic across the world, thanks to a string of high-profile attacks. There is a sense that no one is immune to attacks from a persistent and organised community of cyber-criminals who use ransomware as their main modus operandi.

Some of the most worrying attacks have been those on national infrastructure. During the WannaCry attack, for example, the NHS was seriously affected, facing demands for payments of $300 or $600 per computer to restore access. The disruption led to significant delays in hospitals and surgeries across the country.

Ransomware may be one of the most popular forms of malware today, but this hasn't always been the case. Malware, like any virus, favours threats that can adapt and evolve to their surroundings. As we become more connected and our economy gets more digital, we face a growing threat from cyber-attacks, with ransomware at the heart of modern cyber-criminals' arsenals.

Cyber-vandals to cyber-criminals

The origins of ransomware can be traced as far back as 1989, when unsuspecting victims were infected with the 'AIDS trojan'. This was distributed through floppy disks that were sent to victims via the normal postal service. Although the world was unprepared for such an attack, the virus struggled to spread at the time because few people used personal computers and the Internet was still in its very early stages. In addition to this, encryption technology was still limited back then.

In spite of its early beginnings, ransomware wasn't a popular form of malware in the 1990s and early 2000s as the main aim was to gain notoriety through cyber pranks and vandalism, with hackers using graphics to communicate the attack to the user. These graphics were