Selling Odays by the Pound: Does Responsible Disclosure Work?

Saskia Coplans

@DI_Security

Digita|nterruption.

saskia@digitalinterruption.com

@ms__chief

@InfoSec_Hoppers

@mcrgreyhats

@OwaspMcr

1. What is it and who does it apply to?
2. What does the law say?
3. But there are standards right?
4. Surely vendors want us to disclose?
5. Balls…

1 What is it and who does it apply to?

Responsible Disclosure is a model or process in which a vulnerability or issue is **disclosed** only after a period of time that allows for the vulnerability or issue to be **patched** or **mended**.
It is not a legal binding **contract** that will lead to **payment** for disclosure or a commitment to **patch**. It is not a Bug Bounty programme and will not protect you from **prosecution**.

1 What is it and who does it apply to?

- Security researchers
- Security companies
- Governments
- Coordinators
- Users - *so, basically anyone…*

2 What does the law say?

- There must be knowledge that the intended access was unauthorised; and
- There must have been an intention to secure access to any program or data held in a computer.

NB: The act does not provide a definition of ‘computer’…

3 But there are standards right?

Information technology — Security techniques — Vulnerability disclosure

1 Scope

This International Standard gives guidelines for the disclosure of potential vulnerabilities in products and online services. This International Standard details the methods a vendor should use to address issues related to vulnerability disclosure. This International Standard

a) provides guidelines for vendors on how to receive information about potential vulnerabilities in their products or online services,

b) provides guidelines for vendors on how to disseminate resolution information about vulnerabilities in their products or online services,

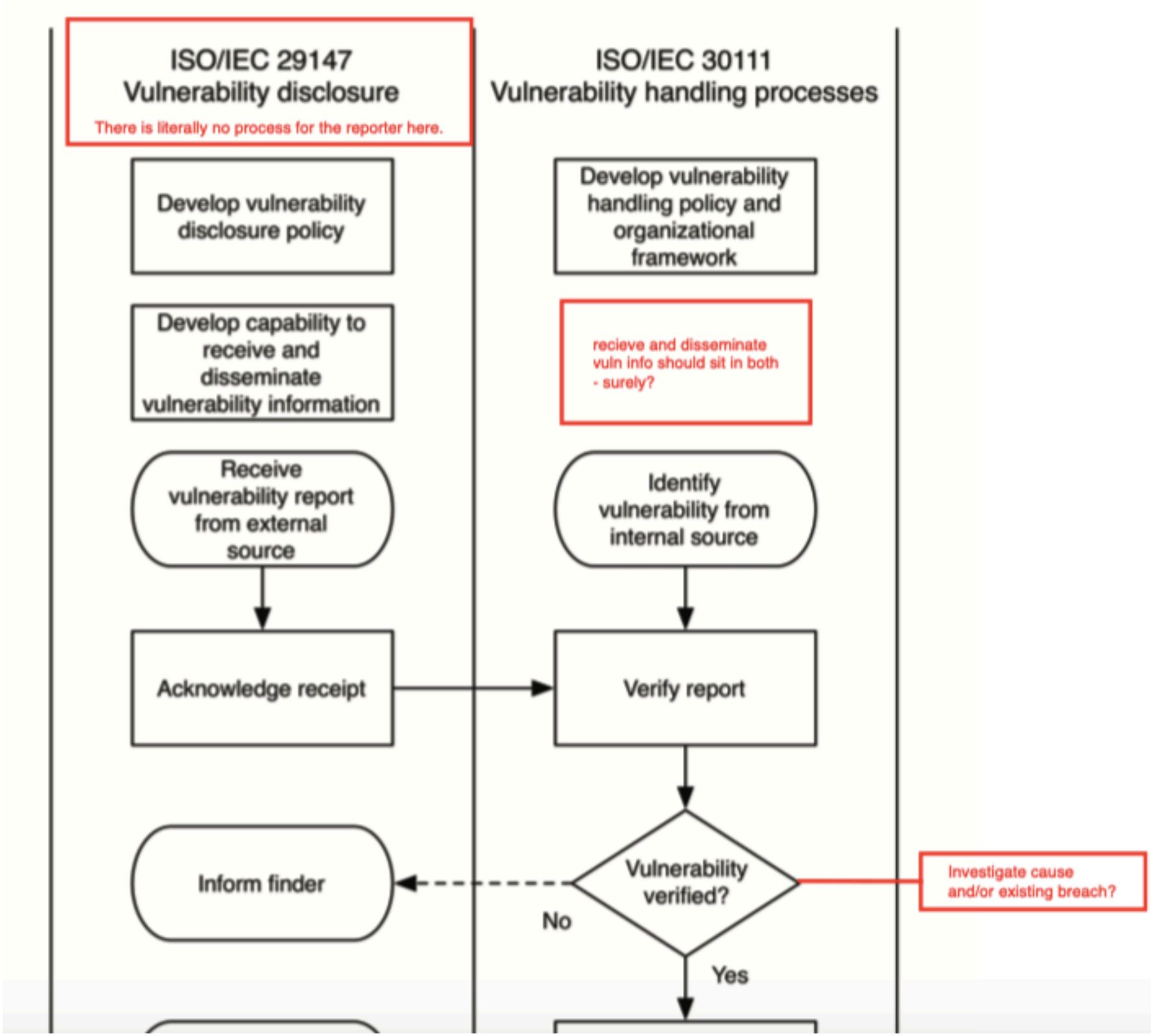
c) provides the information items that should be produced through the implementation of a vendor's vulnerability disclosure process, and

d) provides examples of content that should be included in the information items.

This International Standard is applicable to vendors who respond to external reports of vulnerabilities in their products or online services.

3 But there are standards right?

There are only 2 pages on reporting vulns in a 34 page document. That is titled "disclosure".


ISO/IEC 29147
Vulnerability disclosure
There is literally no process for the reporter here.
Develop vulnerability disclosure policy
Develop capability to receive and disseminate vulnerability information
Receive vulnerability report from external source
Acknowledge receipt
Inform finder
ISO/IEC 30111
Vulnerability handling processes
Develop vulnerability handling policy and organizational framework
recieve and disseminate vuln info should sit in both - surely?
Identify vulnerability from internal source
Verify report
Vulnerability verified?
No
Yes
Investigate cause and/or existing breach?

3 But there are standards right?

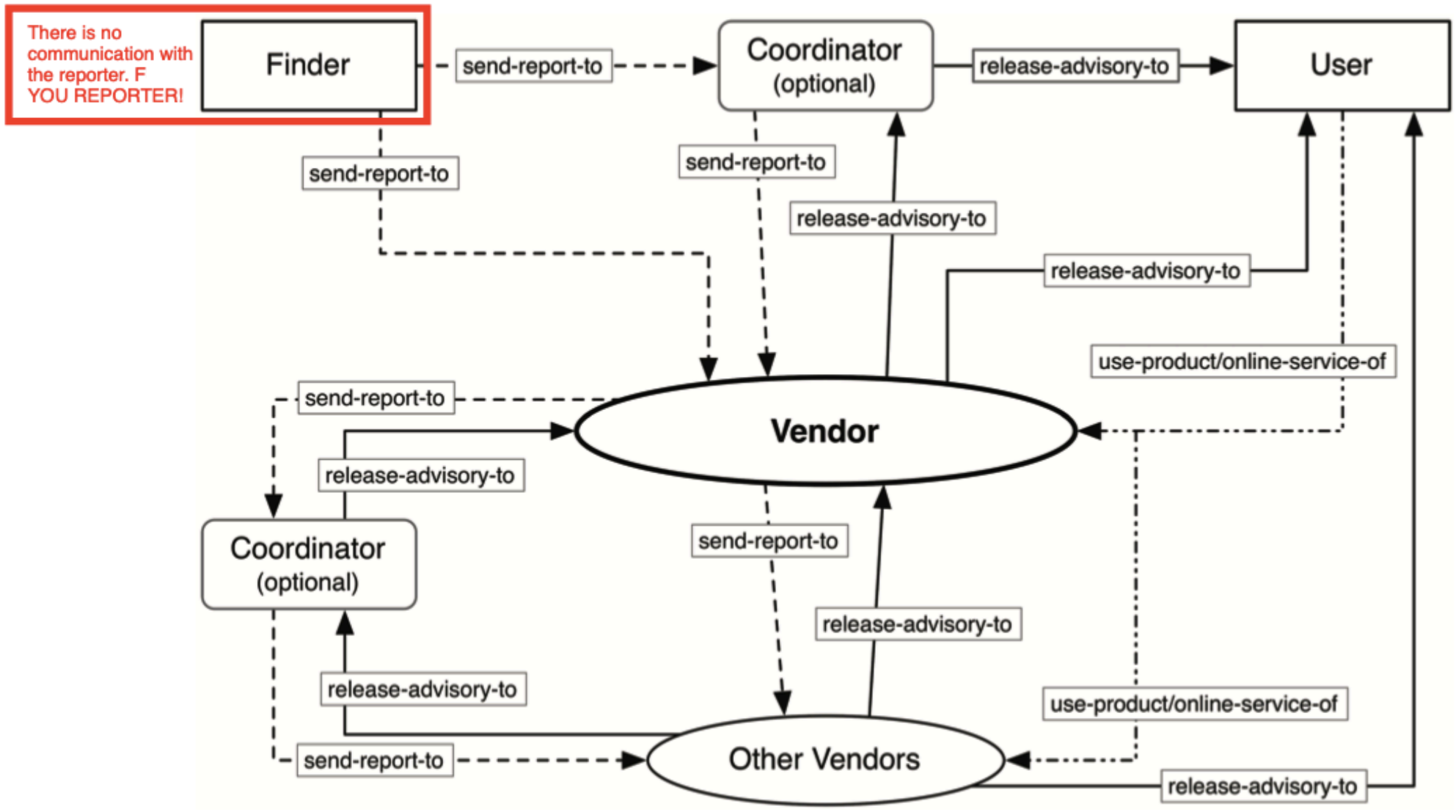


Figure 3 — Vulnerability information exchange

3 But there are standards right?

It is advisable to set out commitments for working together in this partnership. Good arrangements give all the parties more certainty on their respective positions and can contribute to the common goal of increasing the security of information systems. This policy guideline offers organisations a look at how a coherent responsible disclosure policy can be structured so as to facilitate reporting of vulnerabilities in proper cooperation with the ICT security community. For hackers and researchers, it is a method that provides its own safeguards.

What safeguards?

It does not violate applicable criminal law frameworks, but the guideline is meant to offer organisations a tool for working together with all parties that highly value the security of ICT systems in a constructive and custom-tailored policy. This actively contributes to reducing the security risks that vulnerabilities represent and their potential negative societal, economic and financial impact.

So not standard and not legal binding so no safeguards in reality .

I literally write standards and I have no idea what this means.

Fundamental to responsible disclosure is that the parties involved adhere to the arrangements on reporting and dealing with the vulnerability. A party that adopts a responsible disclosure policy may, for example, undertake the obligation to not report a vulnerability if the rules applicable under the policy are not complied with.

The primary actors in responsible disclosure are the discloser and the organisation that is the owner/administrator of the system. It is important to have the minimum possible number of links in the chain between the person disclosing the vulnerability and the organisation responsible for solving the problem. The discloser and the organisation may, however, jointly decide to inform the National Cyber Security Centre (NCSC) or other parties in the ICT security community of the vulnerability, particularly if the vulnerability is not a known vulnerability, so as to prevent or limit the direct and indirect impact of the vulnerability elsewhere. The NCSC seems to be suggesting not using co-ordinators

The discloser of a vulnerability

The implementation of any responsible disclosure policy hinges on the discloser. The discloser has in some way observed a vulnerability and wants to contribute to the security of the information system by revealing the vulnerability so that the organisation can remedy it. The discloser of a vulnerability is responsible for his/her own actions and the way in which he/she discovered the vulnerability. Reporting the vulnerability does not absolve the discloser from criminal investigation and prosecution if the discloser committed a crime in demonstrating the vulnerability. The organisation and the discloser may agree under a responsible disclosure policy that no charges will be filed in regard to specific criminal activities of the discloser. A similar arrangement may be made for civil actions.

4.1 The organisation

Responsible disclosure starts with an organisation that is owner of information systems or the vendor of a product. After all, the owner/vendor has primary responsibility for the information security of the system or product. An important part of this is that the organisation has the choice to adopt and pursue a responsible disclosure policy, to give the organisation an effective approach to resolving vulnerability issues.

By drafting its own responsible disclosure policy, the organisation makes clear how it intends to handle reports of vulnerabilities. As we have seen from the number of parties that have done so already, this can be done as follows:

The organisation drafts a policy for responsible disclosure and makes it publicly accessible.

- The organisation ensures that the threshold for someone wishing to report a vulnerability is low. The method can be standardised, for example, by means of an online form for making reports. The organisation may wish to consider whether anonymous reports should be allowed.
- The organisation sets aside the capacity for an adequate response to any report received.
- The organisation receives the report of a vulnerability and ensures that it is routed as quickly as possible to the department best able to evaluate and act on the report.
- The organisation sends the discloser a confirmation of receipt of the report, preferably digitally signed to emphasize the priority. The organisation and the discloser then enter into contact to discuss the next steps.

[illegible] vulnerabilities is 60 days. Remedying hardware vulnerabilities is much more difficult; for these, a term of six months can be considered reasonable under normal circumstances.

- In consultation between the parties it may be prudent to extend or reduce this term depending on how many systems are dependent on the system with the vulnerability.
- If a vulnerability is difficult or impossible to resolve, or if resolving it will involve high costs, the disclosure and the organisation may agree to not disclose the vulnerability.
- The organisation will keep the discloser and any other stakeholder parties abreast of the progress in the process.
- The organisation may adhere to a policy of giving the discloser credit for the report, if the discloser so desires.
- The organisation may choose to give the discloser some form of remuneration/recognition for reporting a vulnerability in ICT products or services if the discloser followed the rules of the responsible disclosure policy. The amount of the reward may be based on the quality of the disclosure.
- In consultation with the discloser, the organisation may decide to inform the broader ICT community of the vulnerability if it is likely that the vulnerability is more widespread than the organisation itself.
- In the policy, the organisation will express its position on declining to take legal action where the discloser acts in accordance with the policy.

- The discloser must report the vulnerability as quickly as is reasonably possible, to minimise the risk of hostile actors finding it and taking advantage of it. What does as quickly as reasonlbly possible mean? How are they expected to do this if there is no one standard process?
- However, the discloser must do so in a manner that safeguards the confidentiality of the report so that others do not gain access to the information.

- The discloser's response must not be disproportionate, such as:
  - by using social engineering to gain access to the system
  - by building his or her own backdoor in an information system with the intention of then using it to demonstrate the vulnerability, because doing so can cause additional damage and create unnecessary security risks
  - by utilising a vulnerability further than necessary to establish its existence
  - by copying, modifying or deleting data on the system. An alternative for doing so is making a directory listing of the system.
  - by making changes to the system
  - by repeatedly gaining access to the system or sharing access with others
  - by using brute force attacks to gain access to the system. This is not a vulnerability in the strict sense, but rather repeatedly trying out passwords. Perhaps some guidance on propionate response might help us to understand how far we should go to prove an issue?

4.3 The NCSC

Principally, responsible disclosure is a matter for the organisations and the discloser. Nonetheless, the NCSC's task is to promote the use of a responsible disclosure policy. The NCSC can also be part of consultations between the discloser and the organisation in the process of sharing information on the vulnerability with the target group to limit the further security risks the vulnerability represents. If a discloser or potential discloser contacts the NCSC directly, the NCSC will attempt to put the discloser in contact with the organisation.

Where possible the NCSC will use the information obtained on technical vulnerabilities in consultation with organisations and disclosers to pass the information on to the ICT community. This can be done by publicly disclosing a portion of the information, writing or updating a fact sheet or white paper, or informing organisations in a coordinated manner.

- In any situation in which a report is made to the NCSC, the NCSC will attempt to put the discloser/potential discloser into contact with the organisation.

4 Surely vendors want us to disclose?

- Reputational damage
- Risk to functionality of existing software
- Cost
- Don’t know how to fix it
- Might not be able to fix it - (forever day)
- They hate us…

VideoLAN
@videolan

Replying to @Scott_Helme @Sand_Pox and 5 others

Personal opinion: yes, you are overall very bad. We have only negative feedback from interacting with this community.
It is always insults, death threats and clueless people.
And never people who try to talk and discuss.

Jamie Hankins
@2sec4u

"something doesn't use HTTPS"
infosec: "SHUT THIS SHIT DOWN RIGHT NOW. CVSS 10.0"
devs: "but we sign the updates & prevent downgrade attacks"
infosec: "SSL"
devs: "you try managing hundreds of mirrors and getting them all to implement & manage SSL"
infosec: "SSL"

5 Balls…

Computer Misuse Act 1990: Convictions 2010 - 2015

Section 1: Unauthorised access to computer material - **85** Convictions

Section 2: Unauthorised access with intent to commit or facilitate commission of further offences - **45** Convictions

Section 3: Unauthorised modification of computer material - **39** Convictions

Total: 169 Convictions

5 Balls...