University of East Anglia

ISC13D027

Title:	***Security update and computer misuse annual report 2014***
Author:	Raymond Scott (ISD)
Date:	16 January 2014
Circulation:	*ISSC 6 February 2014*
Agenda:	ISC13A002
Version:	Draft v0.1
Status:	Open

Issue

To provide an annual report on activities on IT security including security audits, penetration testing, and the number and type of potential security breaches and complaints about computer misuse investigated by the ISD Information Compliance team.

Recommendation

Recipients are invited:

- To receive the report.

Resource Implications

No change to service is required and therefore there is no impact on resources.

Equality and Diversity

The report has no impact on groups with protected characteristics.

Timing of decisions

No decisions are required.

Further Information

- Raymond Scott (ISD), x3561, r.scott@uea.ac.uk

Background

The Information Compliance team in ISD receives, logs and acts on reports of IT security breaches and non-compliance with the conditions of computer use. Incidents can be reported to the IT helpdesk or directly to the team via the shared mailbox misuse@uea.ac.uk.

IT security is also managed through this team which coordinates security audits and penetration tests of systems (to discover security vulnerabilities).

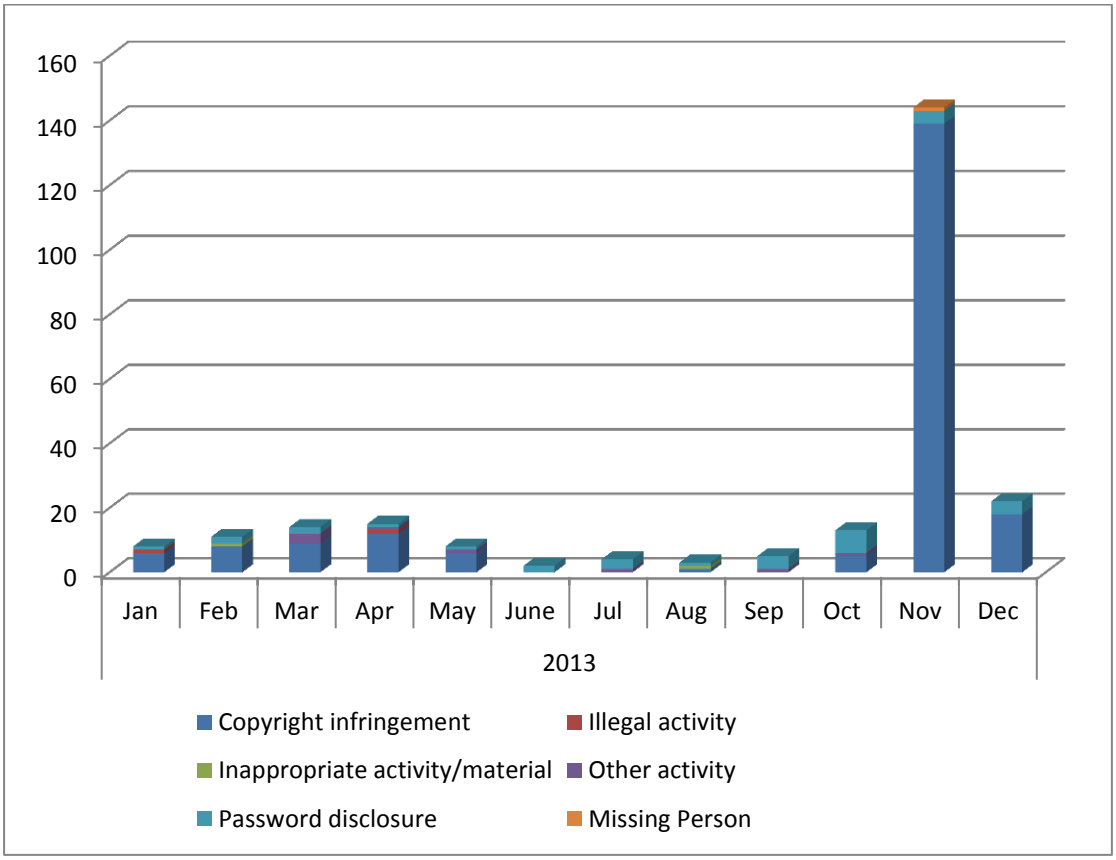
Discussion

Security breaches

The following table shows incidents broken down by category.

Incidents logged, investigated and actioned	2013	2012	2011	2010
Compromised accounts/password disclosures	36	55	7	112
of which repeat offenders:	1	1	3	5
Copyright offences	205	45	127	57
Illegal activity	2	4	0	3
Inappropriate activity/material[1]	2	3	7	
Unauthorised access	-	2	1	
Other	9	4	3	17
Total no. incidents logged and investigated	254	45	145	189

The graph shows the information[2] broken down by month.



During the year, there were significant changes to the way copyright infringements were handled which affected the no. of incidents logged and reported.

- Following RIPE[3] policy, in May 2013, we added the standard RFC abuse@uea.ac.uk address[4] to our WHOIS lookup and wrote to contacts including monitoring agencies

[1] This category was not previously reported, so there is no information held for 2010.
[2] The graph shows a breakdown for records held by the security incident team and held within ESD.
[3] RIPE - Réseaux IP Européens ("European IP Networks")
[4] This abuse address is to be used for reporting network security problems, spam issues, as well as copyright infringement notices among other things.

asking them to update their address books to use the new address to report copyright infringements. (The old cert@uea.ac.uk would be no longer used)

- Arrangements were made for the IT Helpdesk to monitor email sent to abuse and direct it to the correct part of ISD. We noted that coincident with this change in email address, we did experience a drop off in notifications. (This was also coincident with end of term.)
- In October 2013, we reactivated the cert@uea.ac.uk email address so we could make a further attempt to ask monitoring agencies to direct their notices to the correct address.
- The IT Helpdesk logs one call for each email received, so where a monitoring agency generates a large number of notices relating to a single incident, each will be reported individually. Previously, additional (duplicate) reports generated by monitoring agencies did not give rise to additional cases logged by the security incident team.
- The security incident team has arranged with the Helpdesk to add template responses to the call logging system (ESD), and so all copyright infringements are now managed through ESD, and in future monitoring reports will be generated from ESD. For 2013, the report is hybrid of both the old and the new systems.
- For 2014, copyright infringements will be reported separately from other types of incident.

Security audits and penetration testing

The majority of work planned for 2012/13 had been put to hold awaiting the introduction of a new post within ISD of "Information Security Manager". The role holder will provide guidance on risk identification and management, and information security to those developing and delivering IT services. The role holder will lead on IT audits and penetration testing by external companies to check compliance, and investigations into breaches of information regulations and policy, and provide support for investigations by regulatory bodies. This role has now received post release and is currently being advertised. We hope to have someone in post by June 2014.

However, ISD has engaged with Deloitte to undertake an exercise assessing UEA's security maturity against industry recognised good practice framework (CPNI[5] top 20 critical controls) for cyber defence. Deloitte made a series of recommendations for which ISD has responded to in a separate document.

Within 2013/14 ISD, will be undertaking a series of actions as identified in the CPNI report, performing a University wide penetration audit and performing penetration audits on new systems which have been introduced to UEA (DNS/DHCP, ABW, Cloud Hosting and CareerHub). This work will ultimately be co-ordinated by the new post of information security manager. Until they are appointed, the work will be coordinated within the ISD SPC team.

[5] Centre for the Protection of National Infrastructure (http://www.cpni.gov.uk/)