NOTICEBORED

Management briefing on

Comparative security metrics

Executive summary

The management briefing this month concern ways to measure and compare the organization's information security arrangements against others (benchmarking), or against the same organization at some prior point (trends).

Introduction

Generally speaking, 'security' is a relative term. Except perhaps in narrowly-specified theoretical situations, there is no such state as perfectly or absolutely secure but it *is* possible to say that one system, configuration, situation, location, organization *etc*. is more or less secure than another according to various criteria or parameters – and in practice that is generally good enough.

That raises two obvious issues: (1) What criteria or parameters should be used to compare information security? And (2) How should they be compared? This paper primarily addresses the second aspect, the question of how: other awareness papers in this series discuss the wide variety of metrics that are relevant to information security.

The idea of comparing information security between organizations stems from this month's security awareness case study on the Sony hack. Having read and considered the case, it is natural to wonder whether our information security arrangements are any better or worse than Sony's. We'll pick up on that point at the end of this paper.

Potential comparative security metrics

Security benchmarking

Ways of comparing organizations' information security against each other include:

- Formal side-by-side benchmarking studies conducted by consultants, auditors or other unbiased specialists with sufficient access to gather the information, and sufficient capabilities, experience, competence and integrity to identify, measure and compare the subjects fairly and accurately. These are generally the most expensive option but give the most reliable results. To an extent, formalized assessment and certification schemes (such as the PCI QSA, and ISO/IEC 27001 certification);
- Scientifically-designed, unbiased, confidential/anonymized and statistically-significant information security surveys conducted by organizations such as the Information Security Forum which survey a large number of organizations on an equal footing and report back to respondents

on how they scored relative to their peers or all respondents. These are less costly[1] and provide useful comparative data;

- Informal, subjective benchmarking is typified by "That doesn't feel right to me!" Our professional training, expertise, experience and gut feel are commonly the basis for assessing and responding to the situations in which we find ourselves compared to those we have experienced or heard about previously/elsewhere, and our mental models of 'how things should be';
- Generic benchmarking, checking/comparing the organization's information security practices against good practice recommendations made in public surveys, the ISO/IEC 27000, NIST SP800 and other standards, books, articles and reports. These need to be interpreted carefully and applied intelligently, where applicable.

Security trends

Most metrics can usefully be re-measured periodically and the results plotted over time to demonstrate the rate and nature of change, which may in turn indicate improvement or degradation of information security, in effect benchmarking the organization's current against its prior status. A sharp increase in the number of phishing emails detected and blocked by the email security systems since last reported, for instance, may indicate an increase in the corresponding threat and/or improvements in the phishing detection capability. Trends are particularly valuable information security metrics in that they can usually be used to predict the future, whereas most others are purely historical or contemporaneous.

Comparing and contrasting *our* information security against Sony's

Based on our reading of information disclosed and published about the Sony hack, we can identify several information security risks and controls that *appeared* particularly relevant to the incident. Systematically listing and describing them, then reviewing this organization's status against each of them, is one way to compare our information security against Sony's:

Sony	Us
Governance: it appears Sony only appointed a CISO after the Sony Playstation Network hack incident, and his resignation in 2014 perhaps casts some doubt on the support afforded to him by management. The CISO was employed by one of the US companies within Sony group: it is unclear the extent to which his remit and influence extended across the global group.	*[Your notes go here!]*
Strategy: Sony's business decision to go ahead with a film involving a CIA plot to kill the leader of North Korea, despite the predictable angry response and diplomatic incident it caused plus the North Koreans' alleged involvement in the Sony hack, is an example of the interplay between the business and information security. We don't know what might be happening in private but Sony has taken a particularly strong and unforgiving public stance against piracy and extortion, which may have made it a more prominent target for attacks.	

[1] Not free though: on top of the time and effort needed to gather and enter the information into the survey, and to analyse the results, ISF membership (required to participate in the ISF survey) costs thousands of dollars per year!

Sony	Us
Risk management: Sony has been involved in several serious information security incidents, raising doubts about whether Sony management is paying enough attention to, and investing sufficiently in, identifying and treating its information security risks as opposed to all the other risks it faces.	
Network/system security: claims that the hackers had free range on Sony's networks for *months* prior to November 24th during which time they were allegedly able to remove terabytes of data indicates serious flaws in Sony's network/systems security arrangements that both failed to prevent the attack and failed to detect it. On the other hand, competent hackers would have gone to great lengths to gain access, go to ground and conceal their activities. There are *rumors* that the Sony hackers *might* have had help from one or more insiders, emphasizing insider threats – a more-or-less universal concern.	
Incident management: the incident came to a head on November 24th 2014 when a network worm unleashed by the hackers displayed scary images and threats on Sony's computer screens while trashing servers in the background. From that point, Sony's official response took a few days to get up to speed but was quite effective, particularly on the legal side *i.e*. formally notifying current and former employees about the privacy breach and sending out 'cease and desist' letters to the news outlets that were publishing information stolen from Sony. However, an employee (unadvisedly, naïvely and presumably without authorization and against policy) disclosed a screenshot of a hacked computer through social media, stirring up a media storm at the very same time that Sony's crisis and incident management process was ramping up.	
Business continuity: the network worm unleashed on November 24th destroyed or took down a significant part of Sony's IT, severely disrupting its business activities for a substantial period. News reports are unclear about how much, if any, valuable information might have been irretrievably destroyed or lost in the incident but at least one report has indicated that some of Sony's core financial systems will not be fully operational until February, 2 or 3 months after the event.	
Extortion preparedness: Sony *appears* to have refused to comply with the extortion attempt – a brave move considering what is at stake. Again, the decision seems to have been made quite quickly, implying rapid escalation of the issue to senior management, an efficient decision-making process, and strong authority to decide on such an important matter. Calling in the FBI and other experts soon after November 24th further suggests that related activities were rapidly put in motion once the key decisions were made, hinting at Sony having already prepared for something of this nature.	

For more information

Browse the *Security Zone* or contact Information Security for more about the Sony hack and security metrics.