Risk Perception in IT Security
Position Statement

Mary Ellen Zurko
Cisco Systems
1414 Massachusetts Ave.
Boxborough, MA, USA
mez@alum.mit.edu

Mike Lake
Cisco Systems
PO Box 14987
Research Triangle Park, NC, USA
jmlake@cisco.com

ABSTRACT
In this position statement, we relate some of our current thoughts on Security, IT, and Risk Perception.

General Terms
Security, Human Factors.

Keywords
IT Security, Humans, Deployment.

1. INTRODUCTION
While the call for the Workshop on Risk Perception in IT Security and Privacy (RPITSP) emphasizes the perception of risk around end user use of and interaction with IT resources, our particular interests are currently in the area of perception of risk and security of IT workers (operators, administrators, and their management chain) in the context of their job of running (and sometimes securing) an IT environment. As shown in SOUPS programs, posters and proceedings through the years, research in administrators' and operators' use of security and perceptions of risk has been modest [1, 2, 3, 5].

2. SAAS IT
One area of interest and experience we have is the perception of security and risk around IT for Software As A Service (SaaS). Businesses considering the use of SaaS face the question of whether any real or perceived risks change when sanctioned enterprise use of systems extends beyond the boundary of systems owned and managed by the organization's IT. SaaS vendors need to think about what they'll do about perceptions of IT risk. Questions at this level include data center and administrative personnel geography, administrative access to customer data, and notification process in the event of a discovery of a vulnerability or breach. Any lack of alignment with existing compliance, particularly company specific rules, raises questions.

Concretely, potential increase in risk from phishing when the company boundaries are officially extended is one topic of interest. Firewalls can form a layer of defense from use of phished company passwords; similar defenses in multi tenant public SaaS are more difficult. There are several market approaches adopted by SaaS vendors, with varying efficacy at responding to market, customer, and user risk. Extended Validation Certificates provide enhanced user feedback on the quality of authentication of a server, as well as some background vetting. An approach more analogous to firewall protection is to restrict sessions from a particular customer organization to a set of pre defined IP addresses. Issues with that approach include the ability to use the cloud from outside of customer networks, since VPN restrictions, like firewalls, are generally at a lower architectural level than the multi-tenancy in public SaaS. The use of mobile also causes issues with this approach (and so many other established business network security practices). Alternatives such as pre registering intent to use the SaaS outside of the configured IP ranges add both technical and human complexity. The most effective approach may be requiring the use of established Single Sign On technologies, like SAML, on a per organization basis. This allows the customer to continue to control and monitor the use of passwords, including giving the ability to only use them behind company firewalls (or within the company network).

Another sort of human related IT risk in SaaS (as well as elsewhere) is operational deployment and configuration of IT systems [5]. Traditionally there is a strong barrier between development and operations to ensure a form of two-person control. The flip side of this is a lack of appreciation of use cases, work cycle, and complexities of operations. Tools that check that the (security related) configuration is (still) aligned with policy help mitigate the risk of changes through operational user error, and conflicting software installations. Since much of operational compliance tends to be driven by specific detailed requirements, places where tradeoffs need to be considered create difficulties. Unfortunately, security related knobs often require those sorts of considerations.

We note that our experience with perceived risk in SaaS IT has been in the area of mitigating, addressing, and contemplating (as opposed to measuring or researching).

3. NETWORK IT
"Usability" has different connotations for different users, times and contexts. The context of integrating a new vendor device into an existing network presents one set of challenges; of bringing a new customer online, another. Usability always means finding a way to focus maniacally on the user's *goals* rather than simple isolated operations. Enterprise hardware and software today, of both open source and proprietary natures, tend to expose a complex configuration language that must be mastered before the

Symposium on Usable Privacy and Security (SOUPS) 2013, July 24–26, 2013, Newcastle, UK.

security posture of a device or collection of devices can be properly assessed. The proper configuration of devices to achieve relatively simply stated goals requires mastery of a complex configuration model. The complexity appears inherent to the engineer: for example, strong crypto comes at a price, and if the user needs capacity more than strength, the user is going to have to be aware that dropping back from AES-256 to AES-128 (or DES!) to gain additional throughput means an exponential weakening of their crypto. Organizations using that hardware and/or software spend considerable time and effort figuring out how to arrange those simple isolated operations into coherent strategies to achieve, verify, and maintain the business goal in the face of environmental, intentional operational and accidental change. The potential for gaps between the strategies to achieve business goals and the operational realities is one important area of security risk in network IT.

One specific area of current interest is VPN tunnels and considerations around the security of managing them. While VPN tunnels based on either SSL or IPsec technologies are entirely different beasts, with very different management paradigms, they have essentially similar objectives: to allow remote (and perhaps mobile) users to connect safely and securely to a cloistered environment across hostile communications infrastructures, perhaps from compromised or degraded endpoints. We consider some of the use cases and goals to understand potential gaps between them and the raw technology, with an eye towards while might help close those gaps. What are the goals of the operations teams? How do we build systems that understand those goals well enough to detect when those goals are compromised? Does doing so make a system more usable? Does doing so make the basic functionality as expressed in IETF RFCs and service offerings more attuned to the usability needs of its contextualized users?

Looking more closely just at IPsec, we consider the detailed feedback possible on the state of the configuration of an IPsec tunnel. What feedback addresses the risk of mis configuration? Current state? Change history? Time since changes, and what changed? Who made the changes? Different feedback is likely for different roles. "Who and when" seems most likely for operations; current state and previous state for administrators; alignment with separately stated policy or compliance for security officers and management.

On a related basis, we consider what feedback on network activity might enable IT personnel to augment Intrusion Detection Systems (IDS) in detecting categories of (D)DoS or other attacks that current elude tooling. Some visualization or ambient awareness might provide a broader class of detectors than IDS alone, without degrading core personnel performance. We consider this area to be related to emerging notions on how end users can augment security systems [4].

4. ACKNOWLEDGMENTS

Nothing about anything we say has anything to do with what our employers say or sanction.

5. REFERENCES

[1] Jaferian, P., Hawkey, K., Sotirakopoulos, A., Velez-Rojas, M., and Beznosov, K. 2011. Heuristics for Evaluating IT Security Management Tools. Symposium On Usable Privacy and Security. http://cups.cs.cmu.edu/soups/2011/proceedings/a7_Jaferian.pdf.

[2] Johnson, M., Karat, J., Karat, C., and Grueneberg, K. 2010. Optimizing a Policy Authoring Framework for Security and Privacy Policies. Symposium On Usable Privacy and Security. http://cups.cs.cmu.edu/soups/2010/proceedings/a8_johnson.pdf.

[3] Layman, L. and Zazworka, N. 2012. Demo: InViz – Instant Visualization of Security Attacks. Symposium On Usable Privacy and Security. http://cups.cs.cmu.edu/soups/2012/demo/demo01.pdf.

[4] Lipford, H. R. and Zurko, ME. 2012. Someone To Watch Over Me. Proceedings of the New Security Paradigms Workshop.

[5] Wool, A. Trends in Firewall Configuration Errors: Measuring the Holes in Swiss Cheese. 2010. Internet Computing, IEEE (Vol. 14, Issue 4) http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5440153&tag=1.