Pulling Back the Blinders:
Extending IT Security to Physical Threats

Ryk Edelstein & M. E. Kabay

Ryk Edelstein< http://ca.linkedin.com/in/ryked > is CEO of Cicada Security< http://www.cicadasecurity.com > and has served as CEO and lead developer of their Cicada active physical-security technology. What follows is the result of a close collaboration between Ryk and Mich.

* * *

Introduction

The focus of information technology (IT) security practitioners in recent decades has been to secure data systems from unauthorized access and corruption caused by an ever-growing range of logical threats – compromise through the layers of the Open Systems Interconnect (OSI) model.< http://support.microsoft.com/kb/103884 > We implement security measures to protect the back office and the data communications infrastructure through to the client station against known and potential software-based exploits.< http://nvd.nist.gov/ > However, despite the costs and efforts to protect against virtual threats, it seems to me that we expend little effort to protect these systems from physical threats such as theft or tampering A report< http:// www.iofm.com/content/resources/OverallSecuritySpending1.pdf > published in 2011 by the Institute of Finance & Management< http://www.iofm.com > reported on wide differences in spending on physical security within and across industries, with significant proportions of the respondents spending less than 1% of their total budget on physical security. Although many executives reported that they felt that their organization's spending on physical security was adequate, "At the other end of the spectrum, a majority of security executives working in health care facilities, government, and retail feel the amount that is spent on physical security is insufficient to deliver quality asset protection."[p 5]

In the decades when mainframe computers were the norm, physical security.<http://searchsecurity.techtarget.com/definition/physical-security > was immediately recognized as a critical element of IT security. For example, the third edition of the *Computer Security Handbook* published by Wiley in 1995 included explicit sections about physical security; for example,

- Chapter 11: "Hardware Elements of Security"
- Chapter 12 "Computer Facility Protection"
- Appendix 3: "Security Standards Manual Table of Contents (Sample)" which includes 10 headings about physical facility security out of 49 section headings
- Appendix 14: "Federal Information Processing Standards: Abstracts" which points to FIPS PUB 31, "Guidelines for ADP Physical Security and Risk Management" dated June 1974

An industry standard compilation of security policies – Charles Cresson Woods' *Information Security Policies Made Easy*< http://www.informationshield.com/ispmemain.htm > emphasizes the importance of physical-security policies:

> 7.01.01 Physical Security Perimeter
>
> 2. Physical Security Plan
>
> Policy: Every Company X data center must have a physical security plan that is reviewed and updated annually by the senior manager in charge of the facility.
>
> Commentary: This policy explicitly assigns responsibility for the development and updating of data center physical security plans. This policy makes it clear that physical security is a line management responsibility, not a staff department responsibility. This means that physical security must be dealt with in the course of ordinary data center operations, not exclusively by a special group. A special technical group, ordinarily called the Physical Security Department, is generally available for consulting and assistance. In most cases the senior manager in charge of the data center would not actually prepare the plan. Somebody else who reports to the senior manager will typically do this. Some organizations may wish to include words in the policy indicating that this plan will be subject to periodic review by the Internal Audit Department. Good physical security must be in place if good information security is going to be achieved. For example, if anybody off the street can walk into a data center and reboot a machine, then load their own version of the operating system, much if not all of the good work in the information security area will be null and void.
>
> Related Policies: "Critical Business Logic" and "Computer Emergency Response Plans."
>
> Audience: Management
>
> Security Environments: All

Today's Environment

It's hard to secure a laptop, tablet or smart phone that is outside the corporate offices. Encryption, host intrusion prevention, and other end point security technologies are important but they cannot reliably protect a device that is powered on, unattended and unprotected from theft, unauthorized access and tampering. These end-point platforms don't afford the administrator ways of protecting external devices from physical threat.

There are solutions with limited applicability to the general problem of supporting physical security of portable devices. For example, several products provide the ability to encrypt whole disks or to wipe or reset mobile phones, tablets and notebook computers through network connections if their owners report them as lost or stolen:

However, these products suffer from fundamental inadequacies:

- Whole disk encryption provides no benefit to the protection of the data stored on these devices when the device is active, since the encryption works automatically as soon as the authorized users logs on.

- Asset-recovery services, although valuable, are typically invoked only once the owner of the computer has *discovered* the loss or theft. If a service provider can be alerted the moment the event occurs, the system can start tracking sooner and invoke policy-based actions for the protection, transfer, and destruction of data stored on the target asset.

- Physical restraint products cannot ensure usage compliance and cannot report attempted theft or tampering. In any case, they are barely a challenge for a motivated thief.

With federated-identification < http://www.federatedbusiness.org/index.php/faqs > and single-sign-on < http://www.opengroup.org/security/sso/ > strategies playing a greater role in securing our distributed networks, we need to audit and enforce physical security on all connecting stations the moment a threat is detected.

The *Cicada*, from Cicada Security Technology, my Montreal-based company, has been engineered to expand security visibility to the physical level. This patented technology, which was originally designed to provide active protection against asset theft, has proven itself to also be a valuable solution for the protection of any station which hosts confidential information or connects to a secure trusted environment. No larger than a common USB flash storage device, the Cicada is capable of analyzing inputs from a number of trigger sources, and when triggered, instantly invokes both deterrent and protective actions to secure its host station. Triggers include motion, device insertion or removal, insertion of writable media, power and network state changes, amongst other options. .

As I recently wrote< http://cicadasecurity.com/blog/2012/07/expanding-the-vision-of-security-the-importance-of-gaining-visibility-to-physical-threat/ >,

> Once triggered, the Cicada invokes user defined protective actions which can include locking the host to the operating login screen, activating a siren on both the device and the host, dismounting an encrypted volume, and in more extreme cases, brick the host, or even destroy cryptographic keys. As can be imagined, as the protective action occurs the moment the threat is detected, and any information stored on, or is accessible from the active host is instantly protected, and the possibility of exposure of confidential information is minimized.

When deployed as an enabling technology, end-point security platforms make physical threats noticeable and are able to invoke actions defined in their own policies, thus extending their effectiveness to protect the enterprise. At the gateway, authentication policy can be extended to require the presence of an active physical-security device meeting specific policy requirements before the host can be granted access to the trusted environment.

In the case of the Cicada, each device has an embedded indelible serial number which can be used as a secondary authentication factor, enabling the assigned user to be able to roam while carrying both a secondary authentication factor and their physical security technology from station to station. Likewise, as a required component to the authentication process, usage compliance is assured.

The Cicada has been launched for sale with its active monitoring and alerting service. It is currently a participant in the Government of Canada's (GoC's) Canadian Innovation Commercialization program< https://buyandsell.gc.ca/initiatives-and-programs/canadian-innovation-commercialization-program > and is being evaluated by GoC departments.

For more information about the Cicada, see our Website< http://www.cicadasecurity.com/?p=products > and feel free to contact me personally at any time< mailto:ryk@cicadasecurity.com >.

* * *

Ryk Edelstein< mailto:ryk@cicadasecurity.com > *has been actively involved as the CEO of IT networking and security-services companies for over 30 years. He is currently the lead developer and CEO of Cicada Security Technology*< *http://www.cicadasecurity.com/* >*, a Montreal, Quebec based developer of innovative security technologies engineered to protect assets and data against the risk of physical threat. He has been responsible for providing guidance to both public and private sector clients on the protection of their digital assets, and is the co-author of the guide titled "Best Practices for the Destruction of Digital Data"* < http://www.amazon.com/dp/B008UZHQA4>*which addresses current and validated data handling practices for the decommissioning of end-of-life storage hardware using properly aligned technologies.*

[Disclaimer: M. E. Kabay has no involvement in or financial interest in the Cicada product or Cicada Security Technology.]

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *