Government Information Quarterly 33 (2016) 250–257

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

Beyond the Castle Model of cyber-risk and cyber-security

Christian Leuprecht [a,*], David B. Skillicorn [b], Victoria E. Tait [c]

[a] Department of Political Science, Royal Military College of Canada, P.O. Box 17,000, Station Forces, Kingston, Ontario K7K 7B4, Canada
[b] School of Computing, Queen's University, Kingston, Ontario K7L 3N6, Canada
[c] Department of Political Science, Carleton University, B640 Loeb Building, 1125 Colonel By Drive, Ottawa, Ontario K1S 5B6, Canada

ARTICLE INFO

Article history:
Received 13 July 2015
Received in revised form 27 January 2016
Accepted 29 January 2016
Available online 17 February 2016

Keywords:
Cyberdefense
Security
Boundaries
Organizational boundaries
Millennials
Generational differences
Compromised environments

ABSTRACT

The predominant metaphor for secure computing today is modeled on ever higher, ever better layers of walls. This article explains why that approach is as outmoded for cyber security today as it became for physical security centuries ago. Three forces are undermining the Castle Model as a practical security solution. First, organizations themselves tear down their walls and make their gateways more porous because it pays off in terms of better agility and responsiveness – they can do more, faster and better. Second, technological developments increasingly destroy walls from the outside as computation becomes cheaper for attackers, and the implementation of cyberwalls and gateways becomes more complex, and so contains more vulnerabilities to be exploited by the clever and unscrupulous. Third, changes in the way humans and technology interact, exemplified (but not limited to) the Millennial generation, blur and dissolve the concepts of inside and outside, so that distinctions become invisible, or even unwanted, and boundaries become annoyances to be circumvented. A new approach to cyber security is needed: Organizations and individuals need to get used to operating in compromised environments. The article's conclusion hints at more nuanced forms of computation in environments that must be assumed to be potentially compromised.

1. Introduction

The Castle Model is a metaphor for cybersecurity, in which the presence of walls (boundaries), often in layers, create a space that is considered "inside" and, therefore, safe, in contrast to a conceptual "outside" that is considered potentially dangerous. The metaphor draws on conventional castles, with their emphasis on strong walls that are difficult and costly to breach, and gateways that allow traffic out and in, but only in a controlled way that keeps the inside safe.

Walls have a dubious history as tools of defense. From the Stone Age, humans surrounded their settlements by walls, but history is full of examples of 'impregnable' castles being penetrated. The Great Wall of China became irrelevant once China's elite, confronting a peasant rebellion, invited in those same Mongols the Wall had been meant to keep out. Its modern incarnation, the Great Firewall has Chinese spoofing IP addresses to circumvent it. The Maginot line failed to keep the Wehrmacht out of France. The Berlin Wall could not isolate East Germans from the lure of a better life, and was eventually dismantled. The border between the United States and Mexico remains porous, great efforts notwithstanding. The Castle Model of cyber security is as alluring as these physical defenses but, as we shall show, creates an equally false sense of security.

Cyber security and cyber risk are conventionally addressed as technical problems with a small cultural component. We argue that solutions to the rapidly growing problems associated with cyber security require a more balanced understanding. The mindset associated with "defense as walls" risks creating a blind spot to some of the most substantial forces preventing progress in cyber security, forces that are not associated with malignity or laziness, but with the need to get useful and productive work done. Our focus is on the international, national, organizational, and personal forces that are responsible for the present parlous state of cyber security.

Security in the physical world involves social processes. The sociology of surveillance has long shown the same to hold for security in the digital age. Yet, neither surveillance studies nor critical theory has explicitly pondered the social processes that cause an individual to be in/secure in cyberspace, nor the implications that follow. Individuals enter, explore, exploit, and exit cyberspace. It is their nascent, emergent, tentative behavior, and the social processes that ensue, that generate cyber risk in the first place. Luhmann, Giddens, and Habermas observed how risk is related to decision-making: decisions often create largely unintended consequences for others (Leydesdorff, 2010). By virtue of its interconnectivity, unintended consequences can be multiplied several million-fold, and in extremely short timeframes.

The Castle Model for cyber security is marred by a fundamental ethical problem: access to the model is a function of finances, as the degree of protection afforded correlates loosely with sunk costs invested. The rise of the cyber security industry is evidence to that

* Corresponding author.
E-mail addresses: christian.leuprecht@rmc.ca (C. Leuprecht), skill@cs.queensu.ca (D.B. Skillicorn), victoria.e.tait@gmail.com (V.E. Tait).

http://dx.doi.org/10.1016/j.giq.2016.01.012
0740-624X/

effect (Zedner, 2009, chap. 5; Gill, 2006). In many countries, cyberdefense is regarded, at least partially, as a societal good, akin to public health or policing but it is not provisioned in the same way. Instead, the Castle Model directly reinforces the digital divide, and indirectly the digital divide's economic and social fault lines across individuals, households, businesses, geographic areas, class, race, ethnicity, and gender (Castells, 2001; Lu, 2001; National Telecommunications and Information Administration, 1995; Norris, 2001). It also blinds governments and organizations to cooperative opportunities for collective benefit.

Organizations with security concerns normally frame the issue as a dichotomy: "inside" *versus* "outside". What happens inside the organization is permissible; what happens outside is considered to be, at least potentially, harmful or dangerous. This framing applies to countries and their governments (see, for instance, a recent review of US cyber security policy by Harknett & Stever, 2011), to government departments, including the military and security components, to businesses, to other kinds of organizations, and even to households, where land is delineated by property lines, and houses by lockable doors and windows. The difference between "inside" and "outside" delineates the two sides. This separation into inside and outside can also exist recursively within the organization. For example, departments within an organization can have their own "inside" and regard (at least in some sense) the rest of the organization as "outside". This explains, for example, the persistent difficulty of sharing intelligence among organizations within the same government.

No organization can exist as an island. Boundaries must inevitably have gateways that permit resources and information to flow in and out. There is a natural and inevitable tension between walls, preventing access, and gateways, allowing it. This tension reflects the balance between security and usability.

This metaphor of "inside" and "outside" is called the Castle Model (Frincke & Bishop, 2004) because it replicates the medieval mindset: strong (often layered) walls preserving the integrity of the inside against attack from the outside – and the ability to impose strict controls over movement in and out (but often with a curious blind spot to movements within). As in physical castles, walls in cyberspace are costly to build and impede the movement of digital goods, services, and information between the inside and the outside. When these "castles" fail to nest properly, difficult issues present themselves that hint at the fraying of this view of the world. Businesses were once contained inside national borders; the rise of multinational corporations, with their own boundaries that intersect national borders, creates issues that reveal themselves in, for example, the problems that national governments have in adapting taxation regimes to the modern world.

Just as physical castles were built to be imposing, as well as defensible, a great deal of cyberdefense infrastructure adds little to real defense but creates the impression that defenses are in place. This has been called "Security Theater" (a term which Bruce Schneier is credited with having coined). A common example is in the domain of password control. Many organizations insist that passwords contain both upper and lowercase characters as well as symbols. Using this larger character set increases the effective resistance of the password to brute-force cracking by the equivalent of approximately three lowercase characters, a tradeoff that any user of a tablet or phone would happily make. Similarly, many organizations require passwords to be changed regularly. Once an account has been infiltrated, a sophisticated intruder will install a keylogger to capture the new password as soon as it is changed. Furthermore, many users simply change their passwords enough times in succession that their organization's policy allows reuse of the original. Both aspects of password controls are, therefore, largely a form of theater. Although Security Theater is ineffective in increasing actual protection, it remains popular as a way of signaling concern to the wider public.

The problem is aggravated by technologies of protection that are expensive to build; consequently, most organizations buy them off the shelf. This results in defensive monocultures where many different organizations use exactly the same walls. Attackers' sunk costs are thus reduced and optimized as they can invest in one attack technology, knowing that it can be leveraged across many targets. A recent example is the Heartbleed vulnerability, an error that made apparently encrypted communication traffic vulnerable to access by an attacker in a straightforward way. The vulnerability affected, by some estimates, two-thirds of web sites and had serious knock-on effects by invalidating security certificates. Its cause was a programming error that had gone unnoticed for two years in open-source software.

Although all boundaries differentiate inside and outside, they can make this differentiation in multiple ways. Organizations have boundaries in at least three important domains:

The first domain is physical — there are physical or geographical spaces that are defined to be inside the organization. When the organization is a country, this is its territory; when it is a business, this is its workplace (factories, offices, warehouses, and retail space). Boundaries that separate inside and outside in this domain are usually obvious: walls and fences; and gateways and doors to pass through them.

The second domain is temporal — there are times that, at least for businesses, are defined to be inside. We call them the working day. Boundaries in this domain are less obvious, but they are there nevertheless. In some businesses, employees must clock on and off; in others the maintenance of these boundaries is a management task, and employees are expected to seek permission when they will not be "inside" during the normal, expected times.

The third domain is the online world — there are computational and network resources that are considered as inside the organization; and a much larger set that is considered outside. The boundaries in this case are a set of electronic and computational wall technologies that are designed to stop data from moving in and out, except as allowed. The gateways now become more distributed and harder to see, which raises new issues.

Some of these "wall" technologies are:

- antivirus software that examines incoming email and web traffic for the signatures of known attacks;
- firewalls that embody rules about what other kinds of traffic is allowed in and out of the organizational network and individual systems;
- anti-spam software that examines incoming email for messages that are not real communications;
- authentication mechanisms such as passwords that allow only approved users to access the network and systems; and
- exfiltration detectors that examine outgoing data and block any (usually documents) that are intended to remain inside the network.

Authentication mechanisms sufficed for standalone systems. These other cyberwall technologies are the response to systems that are connected to the Internet, making their internal content potentially accessible to anyone on the planet. Even organizations that are not connected to the Internet, for example militaries and security and intelligence organizations that run their own air-gapped "closed" networks, have been forced to admit that they cannot really consider themselves as separate from the larger world. For example, ubiquitous cameras on laptops mean that data can be passed by pointing the camera of a computer on an outside network at the screen of a computer on an inside network; ubiquitous microphones mean that a computer on an outside network can listen to sounds made by a computer on an inside network (even at frequencies inaudible to humans).

Technology enables three new possibilities that did not exist for real-world castles. Defense in-depth historically meant more concentric layers of defenses, but defense in-depth today reflects the fact that defenses are no longer concentric. The first new possibility is that attack scenarios for complex systems can be computed, taking into account the individual vulnerabilities of walls and gateways, and how they can be chained together to create intrusion pathways. These scenarios are