Cyber Crime Threats, Strategies to Overcome, and Future Trends in the Banking Industry

7

Atul Bamrara
Department of School Education, Government of Uttarakhand, India

INTRODUCTION

Cybercrime is a near and present threat for all organizations today. While primarily focused on the consumer and financial services industry for many years, cybercrime definitively made the shift into the enterprises. Cybercriminals are working everyday to create better technology that will lead to larger payoffs (Brown, 2015; Byrne et al., 2002; Broadhurst et al., 2014). They are switching their methods and hitting diversified targets to yield better information. As experienced by one organization: It took cybercriminals just four hours to overcome a countermeasure that had taken them four months to develop. Managing risk against the threat of cybercrime is certainly not easy an easy task (Taylor et al., 2014; Yuan et al., 2016). One of the most important lines of defense is intelligence and awareness of the potential risks and governments have been making great strides to embrace information sharing among competitors and partners, but most importantly, the general public (Bauer et al., 2017).

BACKGROUND

Strategies to Overcome Cyber Threats

When a bank's system is connected to the internet or intranet, an attack could originate anytime, anywhere. Some acceptable level of security must be established before business on the internet can be reliably conducted (Byrne et al., 2002; Bossler et al., 2012; Aboobucker et al., 2018). An attack could be any form like:

- The intruder may gain unauthorized access
- The intruder can destroy, corrupt or otherwise alter data
- The intruder does not gain access, but instead forges messages from user system
- The intruder does not gain access, but instead implements malicious procedures that cause the network to fail, reboot or hang

Modern security techniques have made cracking very difficult but not impossible. Furthermore, if the system is not configured properly or the updated patches are not installed then hackers may crack the system using security hole. A wide range of information regarding security hole and their fixes is freely available on the internet.

DOI: 10.4018/978-1-7998-3473-1.ch086

1. AUTHENTICATION TECHNIQUES

Authentication is the act of establishing genuineness or originality of a subject. It can be divided into many types depending on how it is performed. Authentication techniques evolved and got strengthened by continuous refinements so as to lessen attacks on private domains (Raza et al., 2011).

1.1 Single Factor Authentication

A well-known and trusted solution in the initial days of computerization was validation by a single attribute. It was effective in the days of localized processing and single user environments. But as networking and Internet based applications spread everywhere, and users were required to maintain passwords for many sites and different applications, they tended to use a single password for all applications on different websites (Fernando et al., nd; Shareef et al., 2018). There are several reported cases where attackers broke into low security websites and retrieved thousands of username/password pairs and directly try to use them by trial and error methods to enter high security e-commerce sites such as eBay with the intention of committing frauds.

1.2 Web Password Hashing

PwdHash is a browser extension that transparently converts a user's password into a domain-specific password (Simmons et al., 2006; Frankel et al., 2011). PwdHash automatically replaces the contents of these password fields with a one-way hash of the pair (password, domain-name). This makes the program on the website process only the domain-specific hash of the password, and not the password itself. A break-in at a low security website exposes password hashes rather than an actual password. Though this was a very effective technique, it required extensions to be added to the browsers. This feature if embedded into every browser will avoid the need to install any extensions.

1.3 Two Stage Authentication

All users cannot be expected to load extensions to their passwords as it requires some knowledge of processing and also as password-stealing attacks have become so common that the software industry observed that the two stage authentication may control the ID theft only to some extent (Subsorn et al., 2012). Businesses chose different methods for second stage authentication apart from passwords. The second input for authentication should preferably be dynamic and possessed by the authorized user. One- time passwords given through tokens, transaction numbers over mobile telephones, grids printed on the back of cards, dynamic digits from ATM card numbers, etc., all are entered as a second input for authentication and come in the increasing order of complexity and cost. Though these methods are loosely termed as second-factor authentication in reality these get used as knowledge based inputs and thus can be stolen or shared (Brown, 2015).

1.4 Multifactor Authentication

The FFIEC – Federal Financial Institutions Examination Council, issued supplemental guidance on authentication in August 2006, in which they clarified, "By definition true multifactor authentication