Chapter 9

The Value of Personal Information

K.Y Williams
Walden University, USA

Dana-Marie Thomas
Walden University, USA

Latoya N. Johnson
Walden University, USA

ABSTRACT

Many cyber-attacks that result in data loss can be prevented if the target of the cyber-attack is properly prepared, has the necessary and latest defenses in place, and is constantly monitoring for attacks and intrusions. Whether those cyber-attacks occur as a result of user error; network issues (password files being created and distributed to a list of people); direct assaults (direct intrusion via a designed hack, system flaw, or exploitation of a known network/software issue); or due to an insider-threat (giving a password to a trusted co-worker who then uses it for other means) one aspect of prevention that must be addressed is the need for better security and additional layers of protection on the data that resides on the servers and in computing systems. With up-to-date protocols, reduced access to the system, and compartmentalization of information, it is possible to reduce the amount and type of data that is lost in many cyber-attacks. This chapter explores five types of information that are targeted during cyber-attacks, and discuss why this information is of importance.
INTRODUCTION

With each cyber-attack the amount and type of data that hackers are retrieving is increasing with more vicious, blunt force, direct attacks, and in the accuracy and efficiency of the attacks. Government agencies have noticed that during the past decade the increase in the information targeted by hackers has grown from what was only information found on servers in government agencies to now include information from servers of financial systems and corporate entities. With this increase of cyber-attacks, the nature of the stolen information has increased to include more specific, personal information.

In the past many individuals, organizations, academic institutions, companies, and government agencies generally thought that one individual alone was usually responsible for an attack, and in the past this may have been the case. However, it is no longer plausible to think that a sole individual is responsible for the substantial number of hacks that occurred over the past decade. In fact, it is far more reasonable to think that larger groups of individuals numbering from three to ten (at least) are responsible for the attacks that have occurred on the different companies, financial entities, and government agencies, and depending on the sophistication and complexity of the system, the number of people involved only grows. Interestingly more direct well-coordinated cyber-attacks targeted towards an individual, organization, academic institution, company, and government agency are no longer scarce, and they are becoming commonplace.

With the increase in the number of cyber-attacks, it seems that hackers may have obtained and secured diverse funding sources to support the cyber-attacks. With renewed funding, computational resources, networking, and multimedia/storage resources, hackers are able to achieve the goal(s) of their attacks with more accuracy and efficiency than in previous years. By utilizing the underlying nature and blind spots within digital systems and having a familiarity with the encryptions used within digital systems, advanced coding, and general knowledge of the flaws within operating systems and servers, hackers are finding it easier and easier to access the targeted systems. This makes the timing and type of attack increase with more efficiency, and with each attack it leaves many of the targets even more vulnerable than expected.

As the number of security breaches increase, hackers not only are able to explore systems with each attack, but also may leave ways to get back into a system for future use. With each intrusion into the system, the information that hackers target range from personal to financial to intellectual in nature. Because the type of information obtained during an attack can vary, it is important to keep in mind that the intent of the attack may be based on the motivation of the person or organization who intends to use the information obtained by the hackers, and not necessarily the hackers themselves if it is done for the benefit of a third party. Private information such as Personal Identifying Information (PII), Personal Health Information (PHI), and private data is valuable in a very particular market and to select groups of people/buyers. Financial Information, Credit Information, and Credit History Information will have a different market, such as others who may have a desire of to gain financially, in the immediate future, or the long term. However, intellectual property and discovery information have a very different value and interest to the right company, buyer, or agency. Additionally cyber-attacks and security breaches that target these types of information hold value if the right combination of information is placed together to create a profile or idea of a particular person, or if the goal is to gain financially from a security breach. This chapter explores these types of information, discusses how the information can be used to compromise individuals, organizations, academic institutions, companies, government agencies, and then explores how financial institutions can be affected by such intrusions.