

7-2008

## Securing Network Data

Robert E. Holtfreter  
*Central Washington University, holtfret@cwu.edu*

Follow this and additional works at: <https://digitalcommons.cwu.edu/cobfac>



Part of the [Business Law, Public Responsibility, and Ethics Commons](#), and the [Information Security Commons](#)

---

### Recommended Citation

Holtfreter, R.E. (2008). Securing network data. *The Informant*, 5(2), 40-41.

This Article is brought to you for free and open access by the College of Business at ScholarWorks@CWU. It has been accepted for inclusion in All Faculty Scholarship for the College of Business by an authorized administrator of ScholarWorks@CWU. For more information, please contact [scholarworks@cwu.edu](mailto:scholarworks@cwu.edu).

## Protecting the Security of Network Data

In 2006 the Privacy Rights Clearinghouse reported 327 data breach incidents, 100,453,730 potentially compromised records and 5 identity thieves who were sentenced after defrauding 238 victims. The data breaches were classified as coming from outside hackers, insider malfeasance, human/software incompetence, non-laptop theft and laptop theft.<sup>1</sup>

One of the biggest data breach's occurred at TJX, a major retail store, where hackers intruded their network at two stores and stole over 46 million debit and credit card numbers from more than 100 files over several years.

The purpose of this manuscript is to draw from the literature to present the major issues regarding threats to the security of network data, define internal/external intrusion and provide a list of the common methods of detection and significant established intrusion preventive practices for maximizing internet network data security,

## Threats to the Security of Internet Network Data

According to Data Recovery.com,<sup>2</sup> there are five major common threats to the security of network data. They are:

1. **Denial of service.** Knowing that all servers have limited capacity to handle all server requests, hackers intrude a network by flooding it with more requests than it can handle, which crashes the server. This threat is relatively easy to do but hard to deal with.
2. **IP masquerading simply means being an IP imposter!** Because of poor authentication in the IP Protocol, the server that is attacking your internet network server pretends to be someone else (with a different IP) and, as a result, is able to gain unlawful access to the server being attacked.
3. **Session hijacking.** Session hijacking is an incredibly dangerous network data security threat where the hacker takes control of a user's session, resulting in a very serious security breach in which the hacker could compromise sensitive user data such as passwords or even credit card information. For example, a user may be accessing some mission critical data or making an internet purchase. At that time, a session hijacker takes control of the user session, thereby getting access to the sensitive session data. The user is led to believe that he has been logged out and he logs back in.
4. **Illegal security break-ins.** This is by far the most obvious and dangerous internet network data security threat. Through either missing security patches in software or access to passwords, the attacker is able to pierce the authentication and authorization checks to get access to corporate databases and mission critical files. This internet network data security threat can be resolved only through prevention rather than cure by safeguarding passwords, tougher password rules etc.
5. **Physical access to servers in data centers.** Physical unauthorized access to our data center corporate servers is still the largest threat to internet network data security. Good data centers have network data security protection in the form of fingerprint based authentication and verification of credentials of all operations personnel visiting the data center.

---

<sup>1</sup> "Chronology of Data Breaches 2006", Privacy Rights Clearinghouse, February 1, 2007.

<sup>2</sup> "Internet Network Data Security Basics and Reviews – The Threats, the Cures and the Strategies for Internet Data Security", [www.data-recovery-reviews.com/intrusion-detection-reviews.htm](http://www.data-recovery-reviews.com/intrusion-detection-reviews.htm).

## Intrusion Detection

What do you do if you suspect that your network has been intruded? The answer is intrusion detection, which is the science of detection of malicious activity on a computer network and the basic driver for networking security. Data Recovery.com classifies intrusion detection for networking security into two parts:<sup>3</sup>

1. **Internal intrusion detection** – this is an incident where a misuse or malicious activity exists that compromises network security from within the computer network (typically internal organizational fraud).
2. **External intrusion detection** – this incident involves a hacker or cracker who attacks the computer network from the outside.

There are two general intrusion detection methods.<sup>4</sup>

1. **Out of the ordinary exceptional or anomalous intrusion detection.** This intrusion detection method relies on checking for any new or strange access in the computer network.
2. **Detection based on past patterns of intrusions.** There are some standard patterns of intrusion into computer networks and pattern based intrusion detection relies on checking if some of these intrusion patterns are repeated on computer networks.

## Established Practices for Maximizing Internet Network Data Security

Over the years a number of established practices for maximizing network security have emerged. They are:<sup>5</sup>

1. **Plan for an optimum internet network data security.** To accomplish this, a balance between access to servers and restricted access through network data security should be put in place.
2. **Data center physical security.** A typical good internet data security practice is to outsource the hosting of corporate servers to a data center that can focus on providing great internet network data security, data center disaster recovery, and tough physical data security. This will help to prevent direct access to servers by unauthorized personnel.
3. **Have a well thought out internet data security policy.** What is needed for an internet network data security policy to work is proper buy in from employees, dissemination of internet network data security information handouts to all employees and contractors and proper internet network data security audits.
4. **A key to internet network data security: Update all software with latest patches.** Updating database and operating software will help to reduce the intrusions by hackers as they attempt to exploit the vulnerabilities of packaged software such as the operation system, the database or even specialized packages such as CRM or ERP packages.
5. **Internet network data security firewalls.** Get an industry standard network data security firewall and safeguard your network from unwarranted intrusions. Also, do period audits of your network data security firewall rules so that your internet network data security is not compromised.
6. **Internet network data security backups and safeguard those backups.** Use new network backup strategies such as remote data backups and data replication to take backups regularly, even when your systems are live. Also, safeguard your backups, as careless backup handling could be your biggest network internet data security threat.

## Conclusion

---

<sup>3</sup> "Intrusion Detection Reviews for Networking Security", [www.data-recovery-reviews.com/intrusion-detection-reviews.htm](http://www.data-recovery-reviews.com/intrusion-detection-reviews.htm)

<sup>4</sup> Ibid.

<sup>5</sup> Op.cit. [www.data-recovery-reviews.com/intrusion-detection-reviews.htm](http://www.data-recovery-reviews.com/intrusion-detection-reviews.htm).

Protecting personal data on networks is a major security problem. Hopefully this article will provide useful basic information for law enforcement officials in their investigation of internet network data security related crimes.

#### BIO

Robert E. Holtfreter PhD is the Distinguished Professor of Accounting and Research at Central Washington University. He has published numerous articles on identity theft, debit/credit fraud, security breaches and data mining models. He is a member of the editorial boards for the Journal of Forensic Accounting and the Fraud Magazine. He also writes a column on identity theft for the Fraud Magazine. He can be reached at [holtfret@cwu.edu](mailto:holtfret@cwu.edu)

Robert E. Holtfreter, P.hd  
Department of Accounting  
College of Business  
400 E. University Way  
Central Washington University  
Ellensburg, Washington 98926-7484