Journal of Cases on Information Technology
Volume 19 • Issue 3 • July-September 2017

Cyber InSecurity:
A Post-Mortem Attempt to Assess Cyber Problems from IT and Business Management Perspectives

Angela Hollman, University of Nebraska at Kearney, Kearney, NE, USA
Sonja Bickford, Department of Industrial Technology, University of Nebraska at Kearney, Kearney, NE, USA
Travis Hollman, Hollman Media, LLC, Kearney, NE, USA

ABSTRACT

Jane, a veteran Accounting employee at Sachem Manufacturing, Inc., recently fell victim to a phishing attack that infected her computer with ransomware. Jane then furthered the attack by logging into key company systems perpetuating the problem. A series of frantic phone calls followed as staff from Information Technology (IT) scrambled to understand the problem and put the broken pieces back together. Unfortunately, the damage was too deep and the problem reached out to hinder a meeting that the CEO was having with an important client. Finger pointing, name calling, and head shaking took over the "War Room" as the top executives soon discovered that their managerial, technical, and political shortcomings were more ubiquitous than they cared to admit. The CEO blamed IT for not preventing the situation and for not communicating effectively with management in understandable terms. IT blamed the CEO for limiting necessary technical resources.

KEYWORDS

Business and IT Relationships, Business Management, Cybersecurity, Hacking, Information Technology, IT, Leadership, Ransomware

INTRODUCTION

Based on onsite observations and discussions with Sachem Manufacturing, Inc. in 2016, this case study takes a unique look at a common phishing cyberattack with. Although the case starts simply with a few small problems, the problems quickly escalate as the organization's assets are compromised. This case emphasizes the importance of guaranteeing a sufficient level of technical security, but it also highlights how organization and management communication breakdowns can have a significant impact on an organization's cyber defenses. The case details the negative consequences that result when upper-level management denies the funding of necessary Information Technology projects because it fails to recognize the importance of preventative security initiatives.

CASE STUDY

Jane arrived at her office in Accounting at Sachem Manufacturing, Inc. at precisely 7:58 a.m. She prided herself on always being prompt in her attendance and precise in her attention to details.

DOI: 10.4018/JCIT.2017070104

At 8:00 a.m., she logged onto her local Windows account on her computer by carefully typing the same username (Jane) and password (J@ne1234) that she had typed so many times before over her seven-year tenure at Sachem. Jane smiled thinking about the day when she cleverly discovered a username-password combination that made use of her name and met the company's eight-character password policy—a policy that required a number, a special character, and both lowercase and uppercase letters. Beyond the initial instructions that helped her to create the password, she had never received any other instructions on how to use her computer.

While her computer processed her input and began its normal log in routine, Jane looked around and smugly noted that Susan, the front office receptionist, had arrived again at 8:05 a.m. She was followed by Barb from Human Resources at 8:06 a.m.

Jane became irritated at her own computer's tardiness. It was still loading, probably performing some sort of inane and untimely update. "This figures," she thought. "The silly thing had all night to do the update without me and now it decides to get to work!"

Jane became more vexed with every passing minute. It was now 8:10 a.m. and the computer was still deciding whether or not it was going to display her Windows screen and all the apps she relied on to stay productive and on schedule. "How unusual," she thought. "It has always logged me in within five minutes, even with updates." In fact, in the last year Jane could not remember a time when the computer had not logged in before the arrival of her late-but-consistently-late officemates.

At 8:15 a.m., Jane's computer finally made up its mind and let Jane in. However, she noticed an ominous warning on her screen stating that her personal files had been encrypted. She clicked the "Next" button. A new screen popped up and demanded that Jane pay $199 to retrieve the encrypted files—*her* files! She then closed two more pop-up windows. One window alerted her that the computer's antivirus was out of date. Another stated that she needed to install more Windows updates.

Windows updates took way too long and the antivirus program never properly installed; Jane started ignoring the warnings a few months ago. Who doesn't? She figured Susan and Barb probably installed updates religiously so that they had another excuse to partake in an early coffee break. But Jane was different. She wasn't going to let those inconvenient "advertisements" delay her workday.

Jane tried to access Sachem's accounting files. Again, a pop-up stated that the files were encrypted. Her annoyance elevated to outright aggravation. At 8:20 a.m., Jane reached for the phone to call Steve, a network manager from Information Technology (IT). Jane left him a message asking him to contact her "immediately."

From 8:20am to 8:22am, Jane called Steve again . . . twice . . . and left him two more messages, each one increasing in urgency. Jane then noted that Steve was probably late, again. She knew that he snuck in 30 to 40 minutes late each day through the back door. Jane picked up the new Sachem employee orientation guide that had been left on her desk and began to read it to herself. At least she could edit while she waited for Steve.

EMPLOYMENT ORIENTATION GUIDE – SACHEM MANUFACTURING, INC. COMPANY BACKGROUND

Sachem Manufacturing, Inc. has a 40-year history of specializing in the fabrication and manufacturing of steel buildings and agricultural grain dryers for industrial applications. Recently, Sachem entered the environmental sector with the development of new environmental products for wastewater treatment and secondary containment systems.

Although a large share of its business occurs within a few hundred miles of its Midwest headquarters, Sachem also maintains two international locations along with other domestic subsidiaries and