The Business Cost of Cyber Crime

Cyber-crime is on the rise. According to a new report by Infoblox there has been a 3500% increase in ransomware domains alone in the first quarter of 2016. While this doesn’t necessarily mean a 3500% increase in ransomware attacks, the report is disturbing. In addition, cyber-crime is now the second most reported crime affecting businesses.

Businesses in all sectors face the threat of cyber-crime attacks. In 2013 Target was the victim of cyber-attackers who gained access to the personal information of up to 40 million shoppers. In 2014, Sony was the victim of another cyber-attack, causing loses close to $15 million, in 2015 it was Anthem Health Insurance, and most recently, the Hard Rock hotel had its card payment system breached. These attacks are becoming more persistent, and damaging businesses around the world.

Cyber-crime can hurt businesses in a variety of ways, including reputational damage, legal costs, Intellectual Property theft, and service disruption. According to a report from PWC, 50 organizations polled in their cyber-crime study, 50 reported losses over $5 million, and of these nearly one third reported losses in excess of $100 million. As losses mount, companies are scrambling to get the upper hand on hackers.

Large corporations are catching up to the cyber arms race. After the attack in 2013, Target vowed to spend $100 million to prevent future breaches. More companies than ever are investing in common sense training for personnel, security auditing teams, and better hardware to fend of cyber-attacks. PWC has seen a 30% growth in their Risk Assurance department per year for the past 3 years. All of this points to a growing need for cyber-security professionals in today’s business world.

For the time being, companies must start taking measures to protect themselves from cyber-crime. The Guardian recommends that the first step companies should take is to raise the importance of cyber-crime in the boardroom. Businesses cannot afford to ignore the risk of a cyber-attacks and the huge implications that that would have on profits. Better training is also an important step in stopping attacks before they happen. In a recent Senate panel, Richard Schaeffer, the NSA’s information assurance director, stated that 80 percent of cyber-attacks were preventable with proper protocol training, configuration, and password management. The most common tactic hackers use is social engineering, encouraging employees to give up their passwords by pretending to be an IT worker or manager. Training employees to better recognize and respond to these attacks is simple and can make the difference between secure and insecure data.

To see cyber-attacks visualized, visit <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

Research links:

http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014

<https://www.linkedin.com/pulse/ransomware-domains-increased-3500-q1-2016-stu-sjouwerman?trk=hp-feed-article-title-share>

https://www.wired.com/2009/11/cyber-attacks-preventable/

<http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey/cybercrime.html>

