Straight Talk from the Corner Office

CORANET
WE PUT A FACE TO TECHNOLOGY®

October 2013

Cybercrime -- *a Growing Threat to Your Business*

Welcome again to *Straight Talk*, one of the ways Coranet shares perspectives on important issues and opportunities in network installation services and project management.

The decision maker research that we shared in the last "Spotlight" found that *Technical Excellence* was ranked at the top of the list of issues businesses care about when choosing a preferred technology support partner. For this Fall issue of *Straight Talk*, we'll examine the current state of cybercrime -- a growing threat to companies of all sizes, as well as an area where technical excellence on the part of the support provider can really make a difference in the business outcome of cyber attacks.

Definitionally, cybercrime can be considered to be any criminal activity that takes place over a communications network. Business-oriented cybercrime spans a diverse set of activities -- from computer hacking designed to steal intellectual property or disrupt business operations, to theft of customer data for the purpose of financial fraud or embezzlement. The majority of cybercrime episodes remain hidden from public view, since most companies are reluctant to disclose when their security has been compromised. Disclosed or not, the actual business impact is huge. In a July 2013 article, the Wall Street Journal conservatively estimated that annual financial losses in the U.S. alone top one hundred *billion* dollars.

The *What, How and Why* of Business Cyber Threats

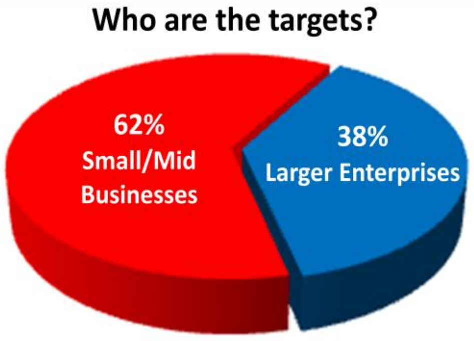
For the past nine years, an annual study of global cybercrime has been conducted by a consortium of prominent security experts from Carnegie Mellon, Europol, Deloitte Risk Management, the U.S. Secret Service, Verizon and thirteen other cybercrime-focused organizations. Their 2013 report studied over 47,000 individual security incidents and provides a clear view of all aspects of business risk associated with cybercrime.

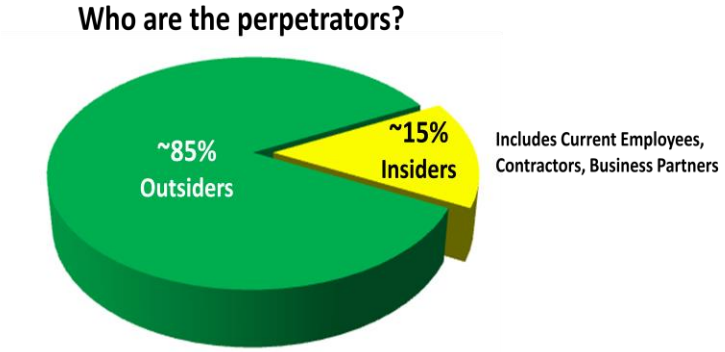
The report opens with a summary statement that goes to the very heart of business preparedness (or lack thereof):

"Some organizations will be a target regardless of what they do, but most become a target because of what they do."

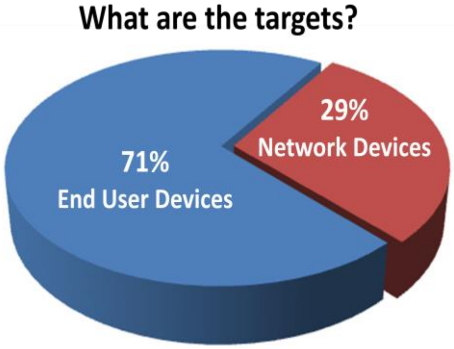
The report makes it clear that every business is at risk -- whether SMB or Fortune 100. While it's usually the big businesses that make the headlines, in fact smaller companies are more frequent targets by far.

Big or small, the bottom line is no business can afford to be complacent when it comes to protecting themselves from cybercrime.

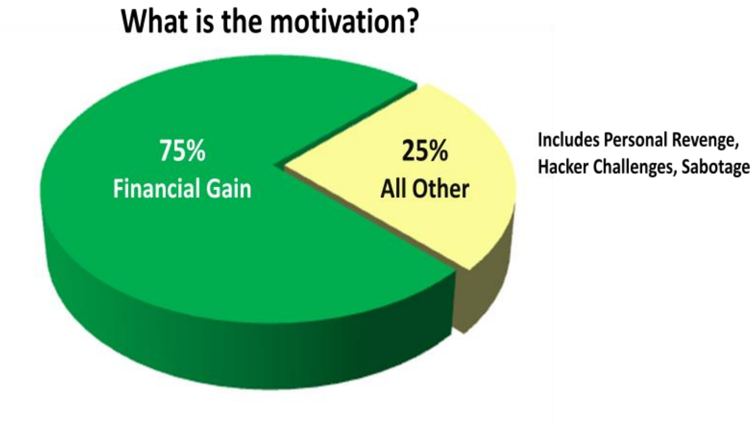




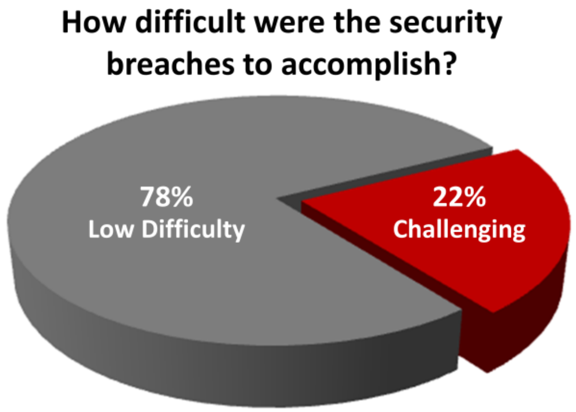
Although the vast majority of security breaches are performed by individuals outside of the firm, the difficult truth is that nearly a fifth of cybercrime episodes are committed by individuals on the inside who have the trust of the business.

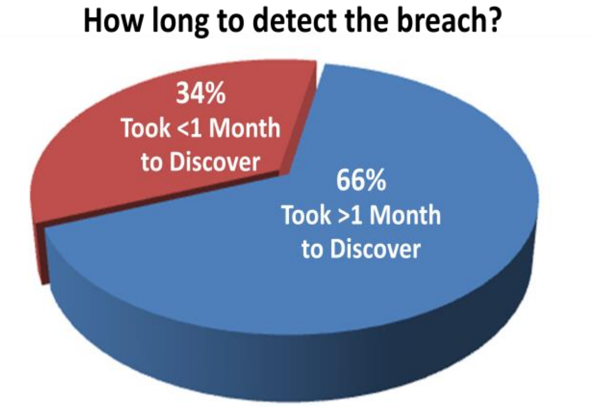


When it comes to the "weakest link" in the business infrastructure, most managers and executives would probably be surprised that their end users represent the overwhelming choice by cyber criminals for "low hanging fruit" -- much more so than network fire walls or routers.



As might be expected, greed remains the driving motivation for the majority or cybercrime episodes, although one out of four incidents had a non-financial motivation, including vengeful employees and ex-employees bent on harassment or sabotage, and bright but misguided computer hackers.





These last two views are particularly telling. As the study experts examined each of the security episodes in their data set, they evaluated how hard it was to compromise the business' security. With nearly 80% of the intrusions being characterized as "low difficulty", the unavoidable conclusion is that most businesses are not well-fortified or equipped to repel security attacks. This take-away is further underscored by the fact that in two thirds of the security intrusions, it took the affected businesses more than one month to recognize that they had been compromised.

How to Avoid Becoming a Cybercrime Casualty

As the cyber criminal element becomes more cunning and ambitious, business security strategies must keep pace. Putting the necessary devices and software applications in place to detect intrusions is clearly a key element in achieving a basic level of business preparedness. But by no means is it by itself adequate to successfully protect your business from attack.

The development and implementation of realistic and up-to-date security policies and procedures provides the essential underpinning for an effective business security approach, as does conducting regular, rigorous assessments of your potential vulnerabilities to external and internal intrusion. As the 2013 cybercrime report emphasized, ensuring an effective level of business protection is a constantly evolving "cat and mouse" situation that requires cutting edge insights on the latest criminal intrusion tactics and malware. Although some IT teams have the all of the specialized internal resources that are required, most firms are likely to need some degree of external expertise to help develop, deploy and manage a comprehensive and effective security solution.

Although we have been focusing on security breaches that take place through communication networks, it is worth noting that an effective business security strategy extends beyond cyber threats and also includes safeguarding the physical security of your sites in terms of entry, access and authentication controls.

In upcoming spotlights, we will examine the specific steps that you can take to protect your business from security vulnerabilities arising from the proliferation of end user mobile devices as well as the adoption of cloud-based services.

Thank you for joining me in this look at cybercrime business risks and ways that you can reduce your company's exposure. I welcome you sharing your reactions, questions and experiences, as well as suggestions for other topics you would like to see covered. If you have any questions, please reach us at questions@coranet.com

Margaret