Testimony of

KEVIN DUNN
TECHNICAL VICE PRESIDENT
PRACTICE DIRECTOR, SECURITY DEFENSE OPERATIONS

NCC GROUP SECURITY SERVICES, INC

Before the

UNITED STATES HOUSE OF REPRESENTATIVES
SMALL BUSINESS COMMITTEE

On

SMALL BUSINESS AND THE FEDERAL GOVERNMENT: HOW CYBER-ATTACKS THREATEN BOTH

April 20, 2016

Good morning Mr. Chairman, Ranking Member Velazquez and other esteemed members of the Committee. Thank you for the opportunity to testify today. My name is Kevin Dunn, Technical Vice President for NCC Group Security Services.

For the last fifteen years I have dedicated my career to carrying out cybersecurity attacks against private companies and government organizations. I am not a criminal; I am a ’Penetration Tester’.

Through our actions in this highly specialized field, my colleagues and I determine ways to break into organizations via cyber and physical means. Specifically, we are hired to identify vulnerabilities that allow a company’s security to be compromised.

This exercise subsequently allows us to provide customized advice to our clients, detailing the short-term and long-term actions they should take to reduce their susceptibility to attack.

My testimony today will focus on four areas:

1. The Strengths & Weaknesses of Cybersecurity Training
2. Increasing Security when using Cloud Service Providers
3. The Potential Impact of Small Business Security on the Government
4. The Benefits of a Data-Driven Risk Model

The Strengths & Weaknesses of Cybersecurity Training

To evaluate the state of high-level cybersecurity training designed for small businesses let's explore two examples: training provided by the U.S Small Business Administration and the Federal Communications Commission.

Through these trainings, small businesses are able to gain awareness of important cybersecurity threats such as the dangers associated with phishing emails, malicious websites, malware, ransomware, and the typical motivations of attackers. This information provides an ample start for educating small businesses in a general awareness capacity, and extends to providing cybersecurity tips for the major areas of concern.

However, the training and guidelines are high-level in nature, and lack the depth of information needed to convert directly into hands-on actions. In the world of small business IT support, where efforts are typically coordinated by owner-operators, this information may not be comprehensive enough to make a worthwhile difference beyond providing general education.

Cybersecurity training for small businesses should provide direct information in the form of 'how-to' guides, answering the need for specific guidance in addition to high-level awareness.

Increasing Security when using Cloud Service Providers

Many small businesses use Cloud Service Providers to implement important services like email, file storage, and data backup. This often unburdens the IT administration overhead from small business owner-operators, or small businesses with a one or two-person IT team.

The use of third party Cloud Service Providers is typically a positive security move for small businesses. The attention to security from the major providers in this space affords a number of features that greatly increase the security of data for a small business. However, it should be noted that there are additional features that should be enabled to make attacks harder for adversaries; these features are often not enabled by default.

Chief among these is the use of multifactor authentication. The majority of major online services now support the use of multifactor authentication, using at least SMS messages to a cell phone as a means of 'out-of-band' authentication. But despite this inexpensive option, it is often overlooked by organizations that use Cloud services, relying instead on 'single factor authentication' in the form of usernames and passwords.

Using multifactor authentication, that makes use of an out-of-band hardware token, would greatly improve security operations for small businesses using Cloud services.

The Potential Impact of Small Business Security on the Government

The impact of a small businesses on the government should be considered in at least two key ways. The first concerns the direct and indirect connectivity between a small business and a Government Network. The second concerns small businesses in the government supply chain.

A small business with a direct connection to a government network is likely a rare occurrence, but in such a scenario if the small business is compromised sufficiently, an attacker's ability to traverse to a government network could be a simple task. However, examples of indirect connectivity are more common and are typically data-based in nature. When government users consume the services of a small business, their usernames, passwords, personal information or other data could be used in a subsequent attack against government systems if extracted from a compromised small business system.

The second area to consider is when a small business is in some way part of the supply chain to a government department or agency. The most typical examples of this are where a small business develops software or hardware that is subsequently installed on government networks.

In all of these examples, if the small business is compromised by a targeted attacker, it could be used as a conduit for gaining access to government systems.

The Benefits of a Data-Driven Risk Model

Finally, a good way to think about security, and a means to ensure that the approaches chosen to secure your organization are ‘fit for purpose’, is to think first about the data that you care about.

Considering the data first is an excellent approach, and one that is advised in the FCC’s Small Business Cyber Planner tool. However, too few organizations actually consider their data, or subsequently plan security around the value of different data types. Even fewer organizations consider what will happen when (not if), an attacker gains access to their data.

Using a data-centric risk management model will allow small businesses to focus their security attention where they need it most.

Thank you again for this opportunity to address the Committee; I will be happy to answer any questions.