CYBERSECURITY ATTACK VECTORS

Ripped From the Headlines!

In 2015, more than 178 million Americans had their records exposed in cyber attacks

****Damage from hacks cost businesses $400 billion per year**

***Cyber attacks cost the average American firm $15.4 million**

**http://www.inc.com/will-yakowicz/cyberattacks-cost-companies-400-billion-each-year.html

*http://money.cnn.com/2015/10/08/technology/cybercrime-cost-business/

FPOV
FUTURE POINT OF VIEW

CYBERSECURITY ATTACK VECTORS

IT'S NOT IF YOU WILL BE ATTACKED BUT WHEN!

There are important ways you can protect yourself and your organization

First, it's vital to understand the major methods cyber criminals use to accomplish attacks…..

FPOV
FUTURE POINT OF VIEW

CYBERSECURITY ATTACK VECTORS

Major Attack Vectors Utilized by Cyber Criminals

Ransomware

Ransomware is becoming more sophisticated and more prevalent. These types of attacks restrict access to a computer until a ransom is paid. If the ransom is not paid, data is destroyed forcing organizations to either pay the ransom or lose critical data forever.

FPOV
FUTURE POINT OF VIEW

CYBERSECURITY ATTACK VECTORS

Major Attack Vectors Utilized by Cyber Criminals

Delivery of Malicious Code

These attacks, often referred to as “watering hole” attacks are characterized by hackers injecting malicious code on to a public web page known to be frequented by those in a particular industry.

This type of attack is intended to infect a computer and thus gain access to a targeted network.

FPOV
FUTURE POINT OF VIEW

CYBERSECURITY ATTACK VECTORS

Major Attack Vectors Utilized by Cyber Criminals

Social Engineering

Individuals are able to prey on the trustworthiness or inexperience of staff by posing as company personnel, vendors, or powerful authorities to gain information or resources that they can use to bypass organizational security.

FPOV
FUTURE POINT OF VIEW

CYBERSECURITY ATTACK VECTORS

Major Attack Vectors Utilized by Cyber Criminals

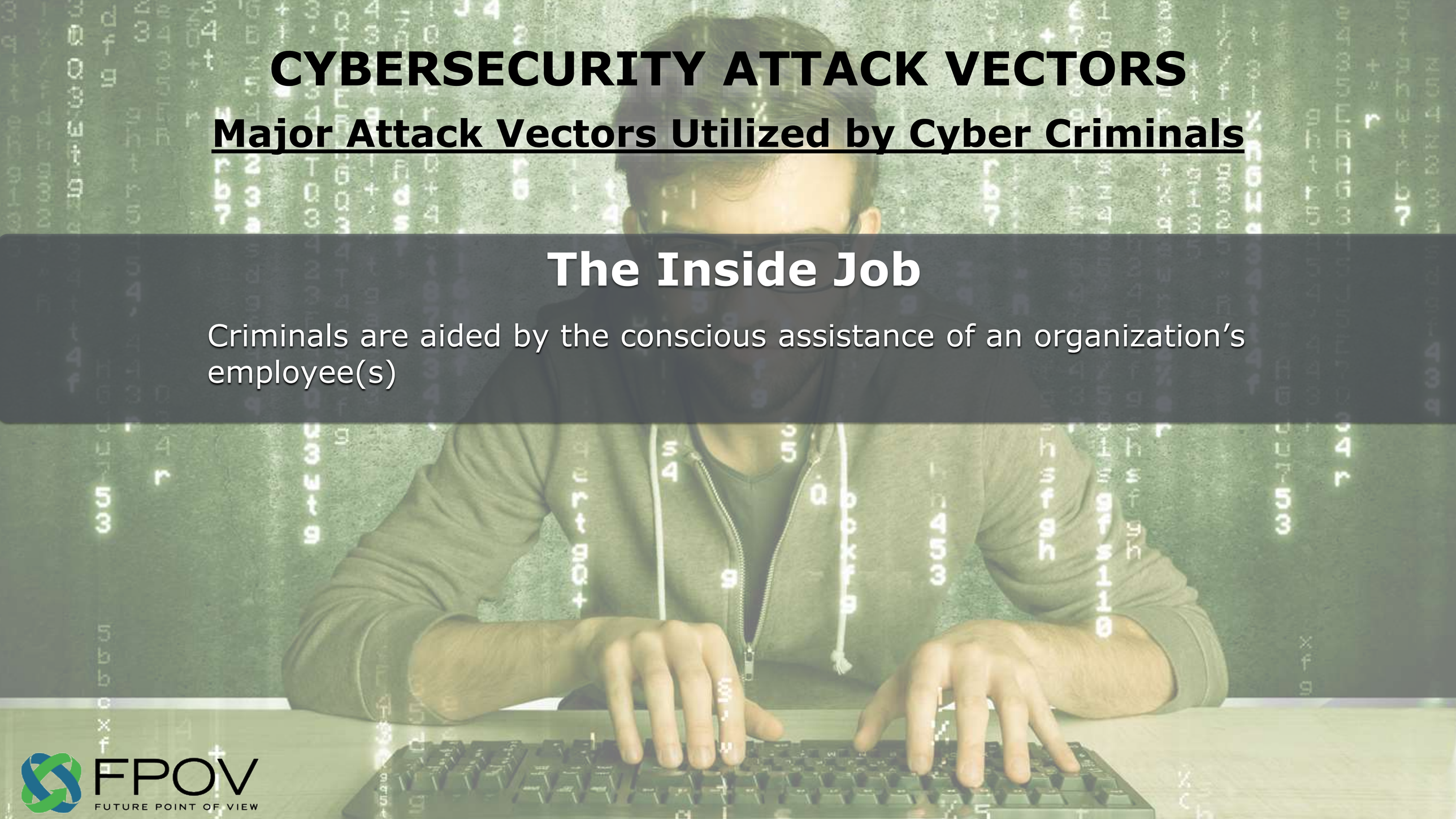
Remote Access

Through open ports or the exploitation of web code, hackers are able to use SQL injection to gain unauthorized access to a server.

FPOV
FUTURE POINT OF VIEW

CYBERSECURITY ATTACK VECTORS

Major Attack Vectors Utilized by Cyber Criminals



The Inside Job

Criminals are aided by the conscious assistance of an organization’s employee(s)

FPOV
FUTURE POINT OF VIEW

CYBERSECURITY ATTACK VECTORS

Major Attack Vectors Utilized by Cyber Criminals

Phishing

Phishing schemes involve attempts to steal your identity or information (such as usernames, passwords, and credit card details) for financial gain by using a fake email disguised as one sent from a trustworthy entity to entice you to click on a bad link or file. These often come dressed as from a financial institution (such as a bank).

FPOV
FUTURE POINT OF VIEW

CYBERSECURITY ATTACK VECTORS

Major Attack Vectors Utilized by Cyber Criminals

Spoofing

The FBI reported that between October of 2013 and August of 2015 $750 million was extracted from more than 7,000 companies using spoofing type scams. Criminals fake correspondance from the executives of victim companies, asking employees to initiate unauthorized international wire transfers on the company's behalf.

In spoofing, an e-mail header is manipulated to look like it came from somewhere different than the source.

FPOV
FUTURE POINT OF VIEW

CYBERSECURITY ATTACK VECTORS

Major Attack Vectors Utilized by Cyber Criminals

Access Through Intermediaries

Retail chain Target suffered an extremely high profile breach in 2013, which led to 40 million credit and debit cards to be stolen during that holiday shopping season.

The attack was implemented in part through the use of a malware that successfully garnered the electronic credentials of Target's HVAC vendor.

FPOV
FUTURE POINT OF VIEW

CYBERSECURITY ATTACK VECTORS

Major Attack Vectors Utilized by Cyber Criminals

Brute Force Attack

An attack that uses automation to systematically check all possible passwords or keys until the correct password is discovered. The success of these attacks are based on the strength of the password. This is why longer, more complex passwords are safer.

FPOV
FUTURE POINT OF VIEW

CYBERSECURITY ATTACK VECTORS

What Can I Do?

There are some important steps you as a leader can take to protect your organization today…

FPOV
FUTURE POINT OF VIEW

CYBERSECURITY ATTACK VECTORS
What Can I Do?

Security Audits & Assessments

These security assessments examine your internal and external security including your firewall ports, packet flow, access and authentication to your network, traffic control and much more. They are followed by a report and a remediation plan that you can use to fix any vulnerabilities.

They should be performed at least once a year. It is also important to do thorough research on any company you will use to perform these. You will be allowing them access to your network, so it is critical that you have vetted their credentials.

FPOV
FUTURE POINT OF VIEW

CYBERSECURITY ATTACK VECTORS
What Can I Do?

Governance

It is important to have procedures and processes surrounding your security including documented rules for passwords, role-based access control, rules for reporting potential security weaknesses, and the requirements for reporting potential security weaknesses and the requirements of applying security updates, patches, and fixes.

FPOV
FUTURE POINT OF VIEW

CYBERSECURITY ATTACK VECTORS
What Can I Do?

Incident Response Plan

Organizations often have documented disaster recovery plans without having security incident response plans. This is unfortunate. Planning for various types of breaches, your organizational response based on the severity of the breach, specific roles during or following a breach, and running exercises that simulate a breach are all important ways you can prepare.

When something does happen you want to ensure that the entire team is working together to mitigate risk.

FPOV
FUTURE POINT OF VIEW

CYBERSECURITY ATTACK VECTORS
What Can I Do?

Education

Your team members can be your greatest asset or vulnerability when it comes to cybersecurity. Every member of your team should be taught how to spot and avoid cyber threats. Security education today must be a cornerstone of every organization’s technology strategy.

FPOV
FUTURE POINT OF VIEW

FUTURE POINT OF VIEW

A Cyber Weapon For Your Organization

Let Us Help You Protect Your Organization
We offer the following services:

INTERNAL ASSESSMENTS: We will assess and report on areas such as Access Controls, Malware, Physical Security, Wireless and Mobile, Change Management, Patch/Update Management, Remote Access, Backups, and Disaster Recovery.

EXTERNAL ASSESSMENTS: Penetration Testing, Network and Firewalls, System Change Management, Public Facing Access, and more.

FPOV
FUTURE POINT OF VIEW

FUTURE POINT OF VIEW

A Cyber Weapon For Your Organization

Let Us Help You Protect Your Organization
We offer the following services:

VULNERABILITY TEST SUBSCRIPTION: These are periodic, random, unannounced, tests to your cyber perimeter to validate that no changes or oversights have occurred that leave your organization vulnerable to an attack or breach.

CYBERSECURITY FORENSICS SERVICE: This is offered if you have already experienced a breach. We uncover and identify where, how, and via whom the breach occurred.

FPOV
FUTURE POINT OF VIEW

FUTURE POINT OF VIEW

A Cyber Weapon For Your Organization

Let Us Help You Protect Your Organization

We offer the following services:

EDUCATION: We offer private and public education to equip your team and leadership with the ability to identify and avoid the latest in cyber threats. These courses are designed to educate all members of your organization how to continually protect the organization's digital assets.

For More Information on our Cybersecurity Education Please Visit FPOV.com/edu

FPOV
FUTURE POINT OF VIEW