Plant Cyber Security

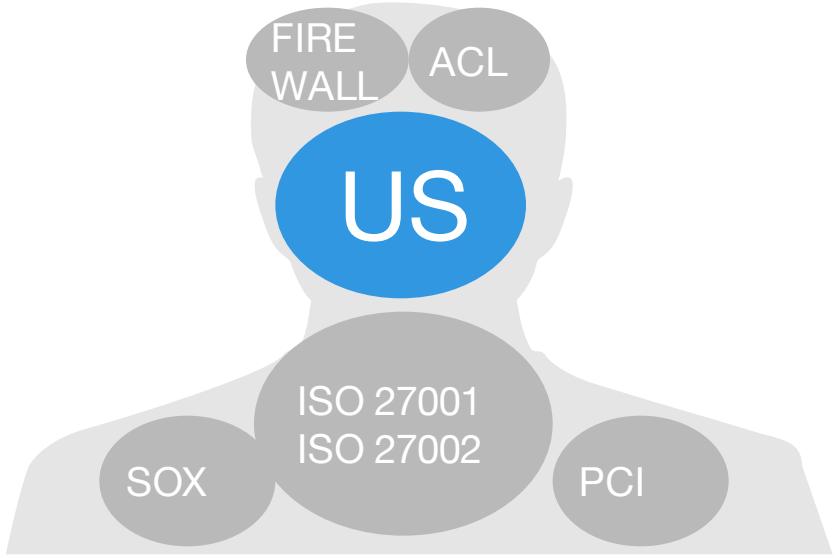
The Rise of Security Analytics

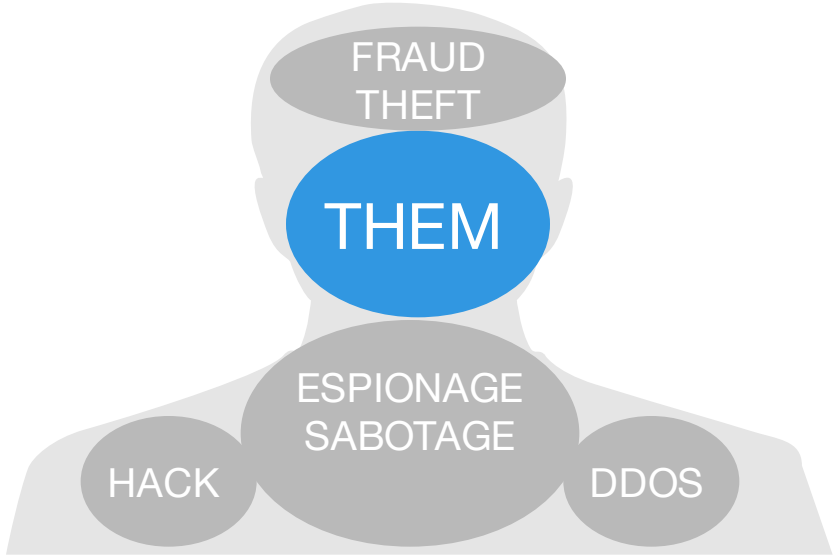
FORENSIC IT
Data Driven Solutions

Purpose of presentation

- In a nutshell, we are going to challenge you to rethink your plant cyber security strategy and make adjustments to protect your plant against future attacks.
- We will give you ideas to secure your plant—and feel that it is secure.
- We will stress to you the value of detecting and acting on intrusions instead of preventing them.
- And yes, we will challenge you to remove virus protection software and malware protection software from your plant computers.

Us vs. Them





IT Manager, Director, CIO

All employees, vendors, contractors, supplementary staff, past and present workers.

Hacker, Cyber Terrorist

Anonymous persons, foreign government sponsored employees and…

…all employees, vendors, contractors, supplementary staff, past and present workers.

Presentation Flow

- First we are going to get our bearings with some definitions and discuss the pros and cons of typical plant cyber security practices.
- Next we will discuss why these methods are always behind the curve and in fact provide a false sense of security.
  - Don't you think that every time you hear about a breach in the news that the company affected most likely had security measures in place?
  - Don't you think that their security measures are probably similar to yours?
  - Don't you think they felt they were prepared?
    - Compliant?

What is plant cyber security?

In general, regardless of industry, the basic definition of plant cyber security is:

"To protect critical digital assets and the information they contain from sabotage or malicious use."

We are going to break this down into its basic parts.

Parts of Plant Cyber Security

DIGITAL ASSETS	SABOTAGE	MALICIOUS USE
• Computers	• Steal Industrial secrets	• Identify theft
• Network Devices	• Disrupt competitor	• Fraud
• Media		• Extortion

What are digital assets?

- Digital assets include and not limited to:
  - Computers
    - Any computer, control room console, laptop, server, hand-held or portable device, personal computer, vendor computer, engineering station, or any other computing device that can access your control system network.
  - Network Devices
    - Any router, switch, hub, or network analysis device that can access your control system network.
  - Storage Devices
    - Any disk, floppy, DVD, CD, USB, internal or external hard drive, flash drive, optical drive, or other storage device that can access your control system network.

What is Sabotage?

- Sabotage has a few different forms:
  - Deliberate action aimed at weakening a corporation through subversion, disruption, or destruction.
  - Stealing of commercial secrets that have real commercial value.
  - Conscious withdrawal of efficiency to cause some change in the workplace.

What is Malicious Use?

- The most common types of malicious use of cyber data are identify theft and fraud.
  - These primarily are associated with personal accounts, retail websites, and back office systems.
- With a manufacturer, what are types of malicious use?
  - Making public corporate secrets, recipes, formulas, manufacturing methodologies.
  - Exposing corporate fraud or wrong doing; flaws in hiring and firing practices, for example.
  - Poor media exposure.

Typical Methods of Protection

- Separation of business systems and manufacturing systems.
- Firewalls to keep intruders out
- Network isolation
- Access Control Lists (ACLs)
- Anti-Virus, spyware, and malware software protection
- Compliance to security standards for IT and Manufacturing
- Password management
- Encryption

Separation of Business and Manufacturing

- Although there is almost always a link between a business network and a manufacturing network, keeping this at a minimum and tightly controlled is a necessity.
  - Unauthorized access to a production network does not mean that business systems are able to be reached.
  - Conversely, unauthorized access to a business system does not mean that the production system, engineering stations, etc., are able to be reached.

Firewalls

- A firewall is a hardware or software appliance that uses rules to allow/deny network traffic based on address, protocol, port, or application.
  - Allow TCP port 135, 443, etc.
  - Deny HTTP port 80
  - Deny Facebook, YouTube, etc. (requires updated Next-Gen firewalls)
  - Allow *.Oracle.com, *.Microsft.com
  - Deny *.somebadsite.com

Network Isolation

- Limit traffic through router and switch configurations to ensure unwanted traffic cannot access specific networks.
- Ensure that a wireless connection cannot access certain systems that a wired connection can.
- Disable interfaces that link networks together that are not used on a routine basis.

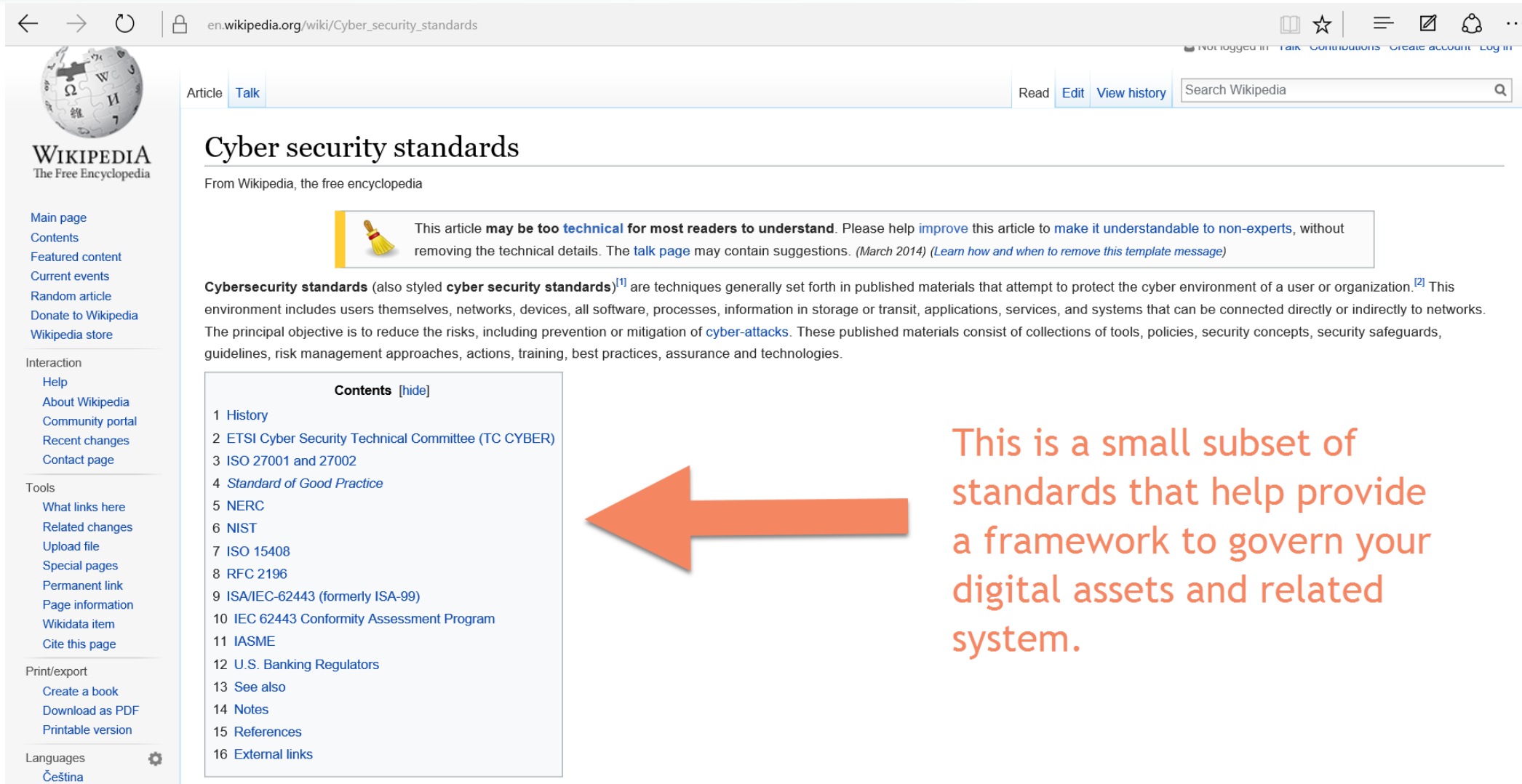
Access Control Lists

- Using groups, roles, and individual permissions, files and data can be protected.
- Most ACLs use and Allow/Deny policy that can accept an object type (group, role, account) to manage permissions.

Anti-Virus, Spyware, and Malware Software

- These packages run on individual systems and use a known database to examine executables and execution signatures against known threats, viruses, spyware, or malware.
- Many offer real-time protection in which they are constantly analyzing signatures, and doing what is referred to as a heuristic checking to look for known bad behavior (i.e., port scanning, email blasts, password cracking, etc.

Compliance to Security Standards



en.wikipedia.org/wiki/Cyber_security_standards

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Create a book
Download as PDF
Printable version

Languages
Čeština

Article | Talk | Read | Edit | View history | Search Wikipedia

Cyber security standards

From Wikipedia, the free encyclopedia

This article **may be too technical for most readers to understand**. Please help improve this article to make it understandable to non-experts, without removing the technical details. The talk page may contain suggestions. *(March 2014) (Learn how and when to remove this template message)*

Cybersecurity standards (also styled **cyber security standards**)[1] are techniques generally set forth in published materials that attempt to protect the cyber environment of a user or organization.[2] This environment includes users themselves, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks. The principal objective is to reduce the risks, including prevention or mitigation of cyber-attacks. These published materials consist of collections of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies.

Contents [hide]

This is a small subset of standards that help provide a framework to govern your digital assets and related system.

Password Management

- Password management includes:
  - Who has access and to what?
  - Password expiration
  - Password complexity rules
  - Keyword rules
  - Clear text or secure transmission.
  - Storage

Encryption

- Encryption can be at numerous levels:
  - Security communication protocols when accessing entities outside your plant (https vs http, for example)
  - Passwords
  - Applications passing secure tokens vs. clear text passwords
  - File systems, directories, files
  - Code

Atypical Methods of Cyber Protection

- Enhanced Password Management
  - The ability to list all users with access to specific digital assets.
    - Who has the enable password to the router?
    - Which users have been given root level access?
  - Password complexity
  - Aggressive password aging
  - Complete access maps (VPN→Firewall→Network Devices→Servers→Applications)
  - Media lockdown (USB, etc.)

Do These Methods Work?

- Ask Google – hacked several times including 5 million gmail accounts
- Ask Yahoo – 2013 over 1 billion accounts, 2014 over 500 million accounts
- Ask E-bay – 2014 over 148 million accounts
- Ask Spotify – 2016, Spotify denies but users confirm credentials online
- Ask Target – 2013 over 40 million credit cards compromised
- Ask Schnucks – 2013 over 2.4 million credit cards compromised
- Ask Iran - 2007 Stuxnet attacked their nuclear fuel program
- Ask Debbie Wasserman Schultz and the DNC!
- According to IBM's 2016 Cyber Security Intelligence report, there was a rise of 66% in the number of manufacturing cybersecurity incidents with a 30% chunk of those being directed at the automotive industry.

So, do these methods work? Yes and No.

Excerpts from McAfee Article June 2014

- … In the US, for example, the government notified 3,000 companies in 2013 that they had been hacked…
- …Two banks in the Persian Gulf lost $45 million in a few hours…
- … A British company reported that it lost $1.3 billion from a single attack…
- …Brazilian banks say their customers lose millions annually to cyberfraud…
- …India's CERT reported that 308,371 websites were hacked between 2011 and June 2013…

https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Article Continued

Most cybercrime incidents go unreported.

Few companies come forward with information on losses.

When Google was hacked in 2010, another 34 Fortune 500 companies in sectors as diverse as information technology and chemicals also lost intellectual property. Some of the information on the incident only came to light from documents made public by WikiLeaks. Only one other company reported that it had been hacked along with Google, and it supplied no details on the effect.

https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Article Continued

Similarly, when a major US bank lost several million dollars in a cyber incident it publicly denied any loss, even when law enforcement and intelligence officials confirmed it in private.

Few of the biggest cybercriminals have been caught or, in many cases, even identified.

https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Forbes Article January 2016

- 'Crime wave' is an understatement when you consider the costs that businesses are suffering as a result of cyber crime. 'Epidemic' is more like it. IBM Corp.'s Chairman, CEO and President, Ginni Rometty, recently said that cyber crime may be the greatest threat to every company in the world.
- Three years ago, the The Wall Street Journal estimated that the cost of cyber crime in the U.S. was approximately $100 billion. The estimate disputed other reports which pegged the numbers by as much as ten times higher.
- In 2015, the British insurance company Lloyd's estimated that cyber attacks cost businesses as much as $400 billion a year, which includes direct damage plus post-attack disruption to the normal course of business. Some vendor and media forecasts over the past year put the cybercrime figure as high as $500 billion and more.

https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#1a127b6b3a91

Forbes Article January 2016 (cont.)

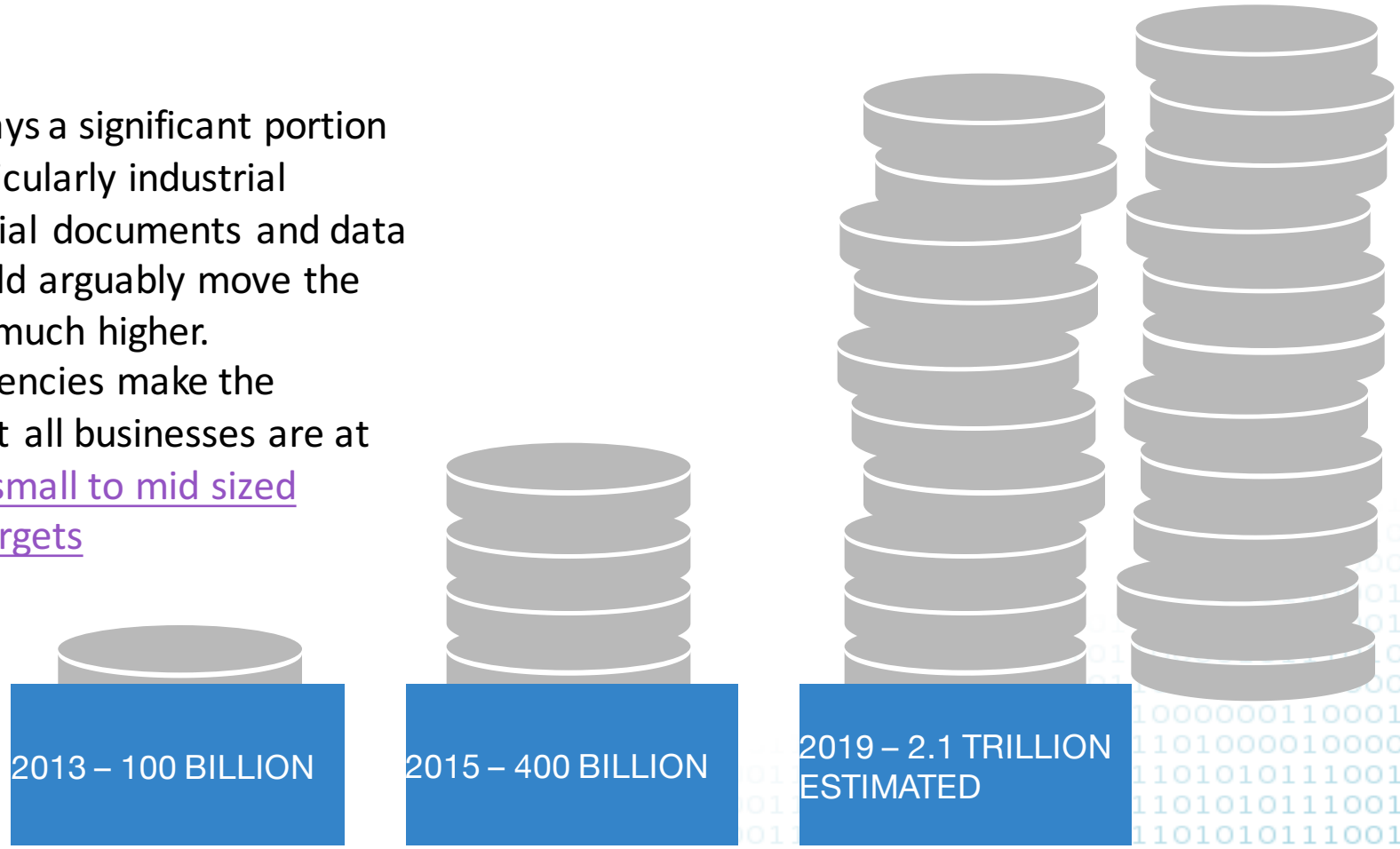
- From 2013 to 2015 the cyber crime costs quadrupled, and it looks like there will be another quadrupling from 2015 to 2019. Juniper research recently predicted that the rapid digitization of consumers' lives and enterprise records will increase the cost of data breaches to $2.1 trillion globally by 2019, increasing to almost four times the estimated cost of breaches in 2015.
- The World Economic Forum (WEF) says a significant portion of cybercrime goes undetected, particularly industrial espionage where access to confidential documents and data is difficult to spot. Those crimes would arguably move the needle on the cyber crime numbers much higher.
- Large banks, retailers, and federal agencies make the headlines when they are hacked - but all businesses are at risk. According to Microsoft, 20% of small to mid sized businesses have been cyber crime targets

https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#1a127b6b3a91

Look At The Numbers

From Previous Slide:

- The World Economic Forum (WEF) says a significant portion of cybercrime goes undetected, particularly industrial espionage where access to confidential documents and data is difficult to spot. Those crimes would arguably move the needle on the cyber crime numbers much higher.
- Large banks, retailers, and federal agencies make the headlines when they are hacked - but all businesses are at risk. According to Microsoft, 20% of small to mid sized businesses have been cyber crime targets



This is staggering

Re-ask the Question: Do they work?

- Earlier we said yes and no.
  - **Yes** they stop some attacks, but, **No**, there is no guarantee with any system to avoid all cyber crime.
  - From the numbers it is clear that even though we have firewalls, compliance, anti-virus software, and have adequately analyzed our risks—the attacks still succeed.
    - This is partly due to the nature of the prevention software.

Why is it such a staggering rise?

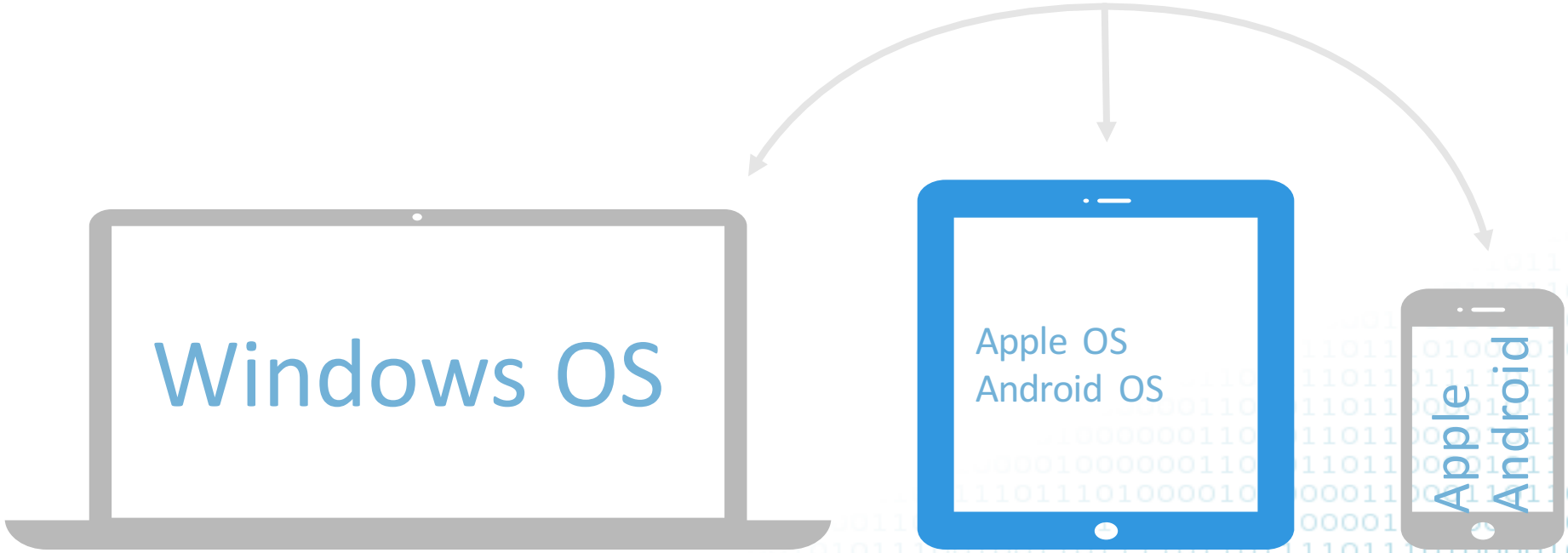
- There are several reasons:
  - More and more businesses have online presences.
  - Within businesses, the desire to connect the business to the manufacturing for scheduling systems, analytics, costs of production, mean that more and more devices and systems are interconnected.
  - Social interaction and phishing
  - Uninformed employees
  - Poor management of resources and digital assets
  - Blacklisting vs. Whitelisting

Interconnection and Data Sharing

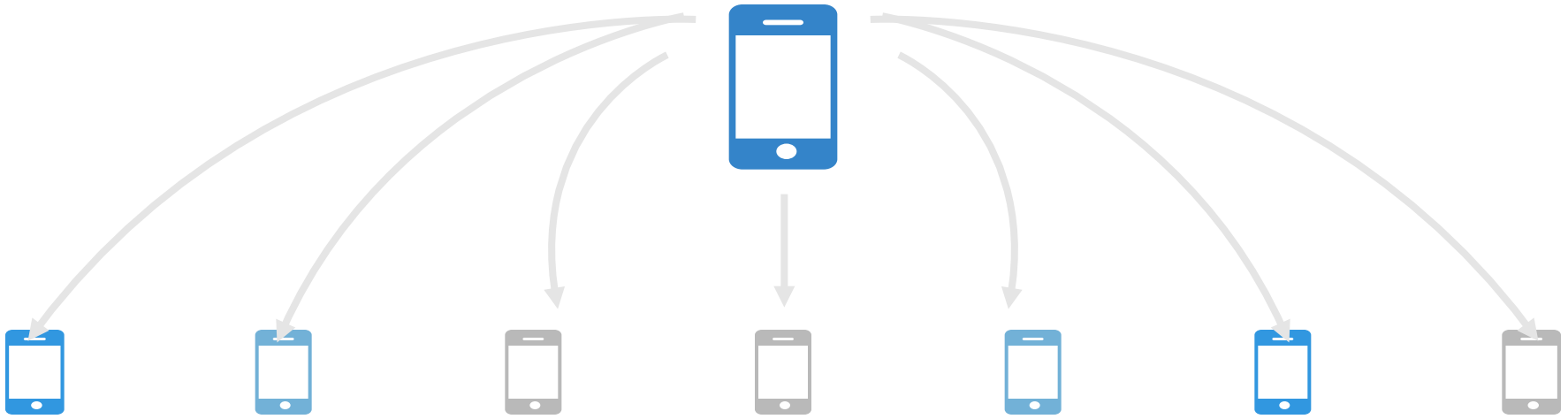
Multiple Platforms, Multiple Code Streams

Cross-Platform

The idea of data everywhere and data on any device is great conceptually, however, it is a nightmare for the security analyst.



Social Interaction



We are so interconnected today that just a whiff of news is instantaneously spread around the globe.

Imagine unfounded rumors and brand damage. "I heard there was a massive data breach at Acme, Inc." Whether true or not is irrelevant. If you were going to purchase from Acme, Inc. you are now thinking twice.

Phishing

- A Bing search of phishing shows the following definition:

  Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. The word is a neologism created as a homophone of fishing due to the similarity of using a bait in an attempt to catch a victim.

- Sometimes it is subtle:
  - “I am doing a survey for a paper, which accounting system do you use? A, B, or C?
  - “Do you use Siemens or Rockwell to control your…?”

Uninformed Employees

- How many of your employees would pick up a USB drive next to their car and plug it into their work computer?
  - Using booby-trapped USB flash drives is a classic hacker technique. But how effective is it really?
    - A group of researchers at the University of Illinois decided to find out, dropping 297 USB sticks on the school's Urbana-Champaign campus last year.
    - As it turns out, it really works.
    - In a new study, the researchers estimate that at least 48 percent of people will pick up a random USB stick, plug it into their computers, and open files contained in them. Moreover, practically all of the drives (98 percent) were picked up or moved from their original drop location.

Poor Management of Digital Assets

- When was the last time you have had a penetration test done to your plant?
- Do you really feel you have a grasp of which users have access to what? Not just employees, but contractor resources.
- User account passwords are changed regularly but what about system passwords, router-enable passwords, network switch passwords, database passwords, ftp passwords? These are rarely changed on a regular basis.
- Do you change all passwords when someone leaves?
- Do you notify all employees that a user is no longer employed?
- How often do you patch your systems and update virus definitions? Best case is usually every 30 days.
- Do you do compliance testing and quickly follow-up on deficient items?

Blacklisting vs. Whitelisting

- Blacklisting software is the typical way most anti-virus, spyware, and malware software work—they scan for “known” offenders. Some look for bad behavior, however, the best case is looking for already known signatures.
- Whitelisting software is total control over what software and executables are allowed to run on a system. A hacker can’t just execute software since it is halted before it is executed.

Blacklisting is OK, but Whitelisting is the only way to go for production manufacturing systems.

Would You Blacklist Access to Your Home?

- In other words, as people entered, you would run a background check looking for criminal activity or other bad activity. You might also implement some heuristic methods and kick someone out who was rummaging through your desk drawer.
  - No, you would not do this.
- You whitelist access to your home. You have absolute authority to control who comes in and who is allowed to stay. There is no unauthorized access.
- In the event of an intrusion, you don't sit by and wait for an anti-virus update (i.e., the police). No, you pick up a bat or other weapon and defend your home.

Anti-Virus, Spyware, and Malware Under Attack

We get these emails all the time from notable anti-virus companies:

Symantec has recently become aware of a medium vulnerability in older versions of the server agent. The latest version addresses this vulnerability in new installations and was released February 15th, 2017. Server agents that are not already upgraded will be identified in the SEP SBE cloud management console starting on March 8th. A manual upgrade will be required to ensure you have the latest protection.

You can take immediate action to manually update to the latest version of the server agent for the Symantec Endpoint Protection Small Business Edition. For more information please see:
https://support.symantec.com/en_US/article.HOWTO124395.html

If you do not take action, we will be releasing a LiveUpdate for server agents beginning in April. Another notice will be sent closer to the LU date.

More information about this vulnerability can be found here:
https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20170306_00

Note: Existing redistributable packages will be deprecated on March 8th and you will need to generate new ones.

The Symantec Customer Communications Team

Article from Microsoft

- An article from the Microsoft Security Team says that "…industry reports show advanced cyber-attacks can go undetected for approximately…

  200 days…".

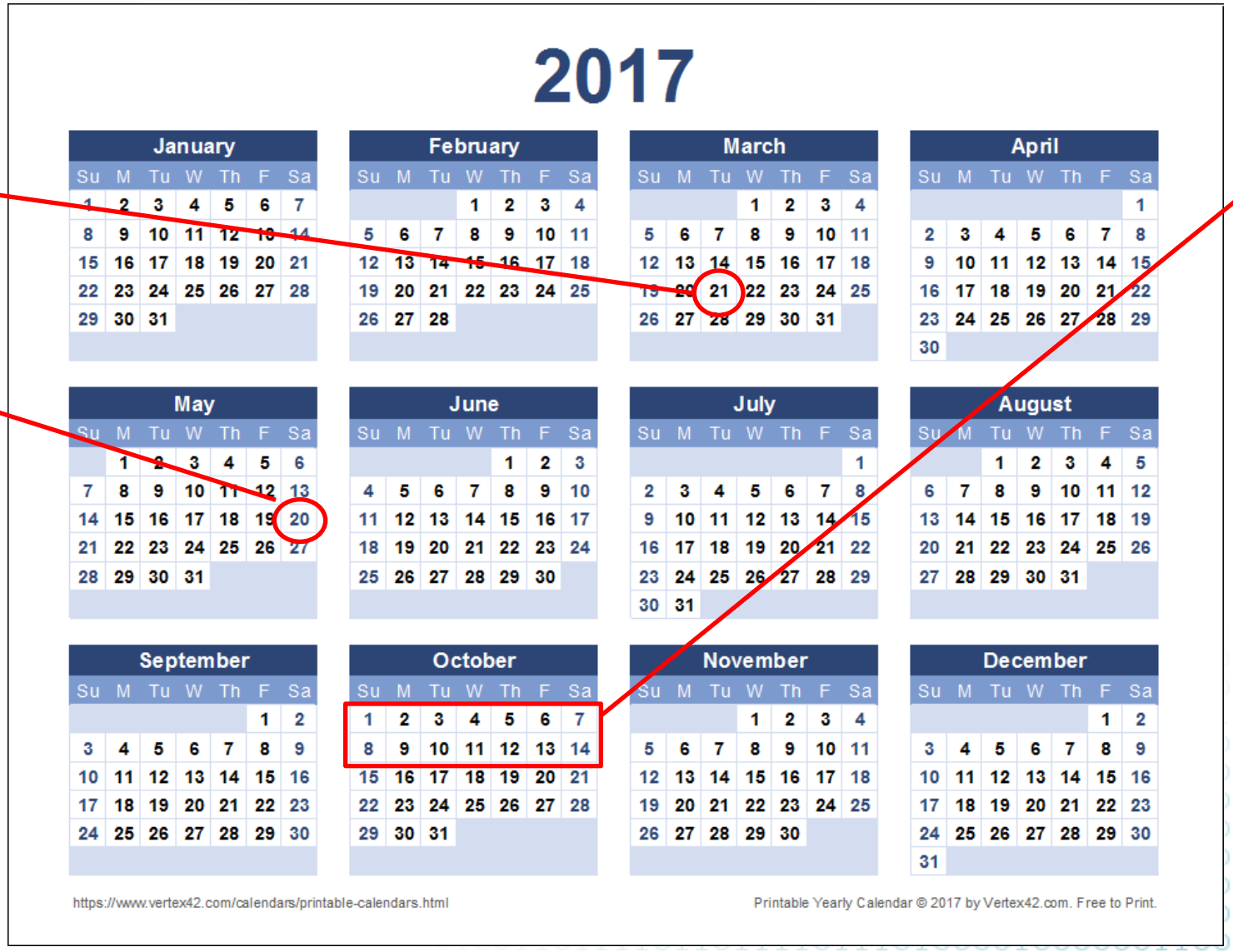
- It is hard to fathom, for 6.5 months, a cyber criminal might be lurking within your systems, extracting data, stealing secrets, etc., all while you feel your systems are protected because you have done everything right.

https://info.microsoft.com/rs/157-GQE-382/images/EN-MSFT-SCRTY-CNTNT-Intelligent%20Security%20e-book%20-%20Lockheed%20Martin.pdfht.

What does 200 days look like?

Infected Today

60 day mark…virus has been running, gathering data, capturing passwords, and transmitting data…for 60 days!



According to Microsoft Security Experts, this is typically the first time your anti-virus software will detect, notify, and protect against the virus. This is the end of the 200 day window.

Sounds Like You Have No Control

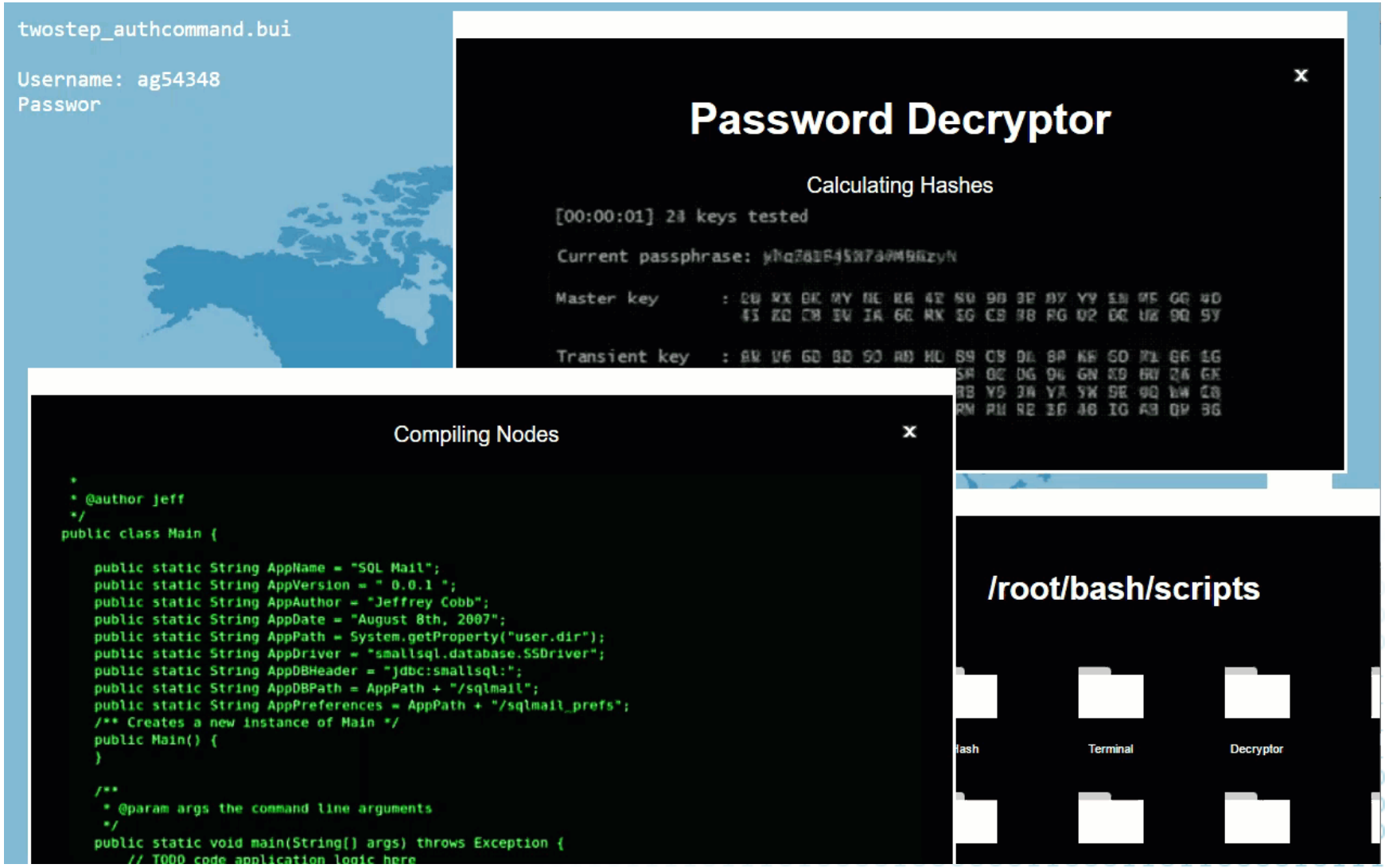
Quite the contrary. You always have control if you <u>just take it</u>.

We will present you with two different options.

- **<u>Option 1</u>** - Stay the course and be part of the 2.1 Trillion in cyber crime statistics that are predicted by 2019.
- **<u>Option 2</u>** – Take control of your production systems and lock them down totally, start using security analytics to be proactive instead of reactive…and yes, remove your anti-virus, spyware, and malware software after you implement whitelist software and Change Management.

Be Realistic – This situation is not yours

Hollywood's Hacker – Probably Not Your Hacker Either



A Dose of Reality

- Part of any cyber security strategy has to involve a comprehensive risk assessment.
  - Although we are all proud of our products and businesses, let's examine the risk.
    - If you make twisty-ties for bread, you are probably at a much lower level of risk than a financial institution or large retailer, but if you make military grade chemicals you are at a higher risk.
    - HP or IBM both provide network management services to other organizations; they are at a higher risk than your average local IT organization that does the same thing.

…But Everyone is At Risk

At Forensic IT, on our first day in a new office, a user plugged in a server to the internet connection to finish configuring it remotely (note: the firewall was delayed but user wanted to configure software).

Within 12 hours the Administrator password was hacked. We determined it was an automated hack from China.

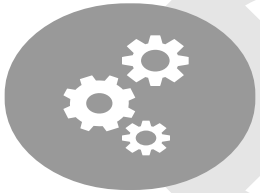
A simple fix is to install the firewall and configure security appropriately, but still…a little scary. There were no goods to obtain, it was just a BOT/script running and trying to plant seeds for later. Luckily we had the skills to fix and remove all traces.

Roadmap to Cyber Security

Finish

Change Management and total system access control.

Step 4

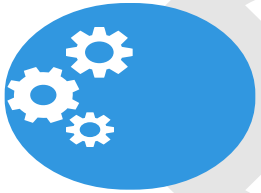


Implement Whitelist software (parallel or replace). Implement mechanisms to gather and use Security Analytics.

Consult security professionals, hire a person, or firm. Take it seriously. Get PEN Tested. Keep deadlines.

Step 3

Step 2



Document all systems, security mechanisms, backup schemes, disaster recover plans, etc.

Start

Assess your risk. Identify all vulnerabilities.

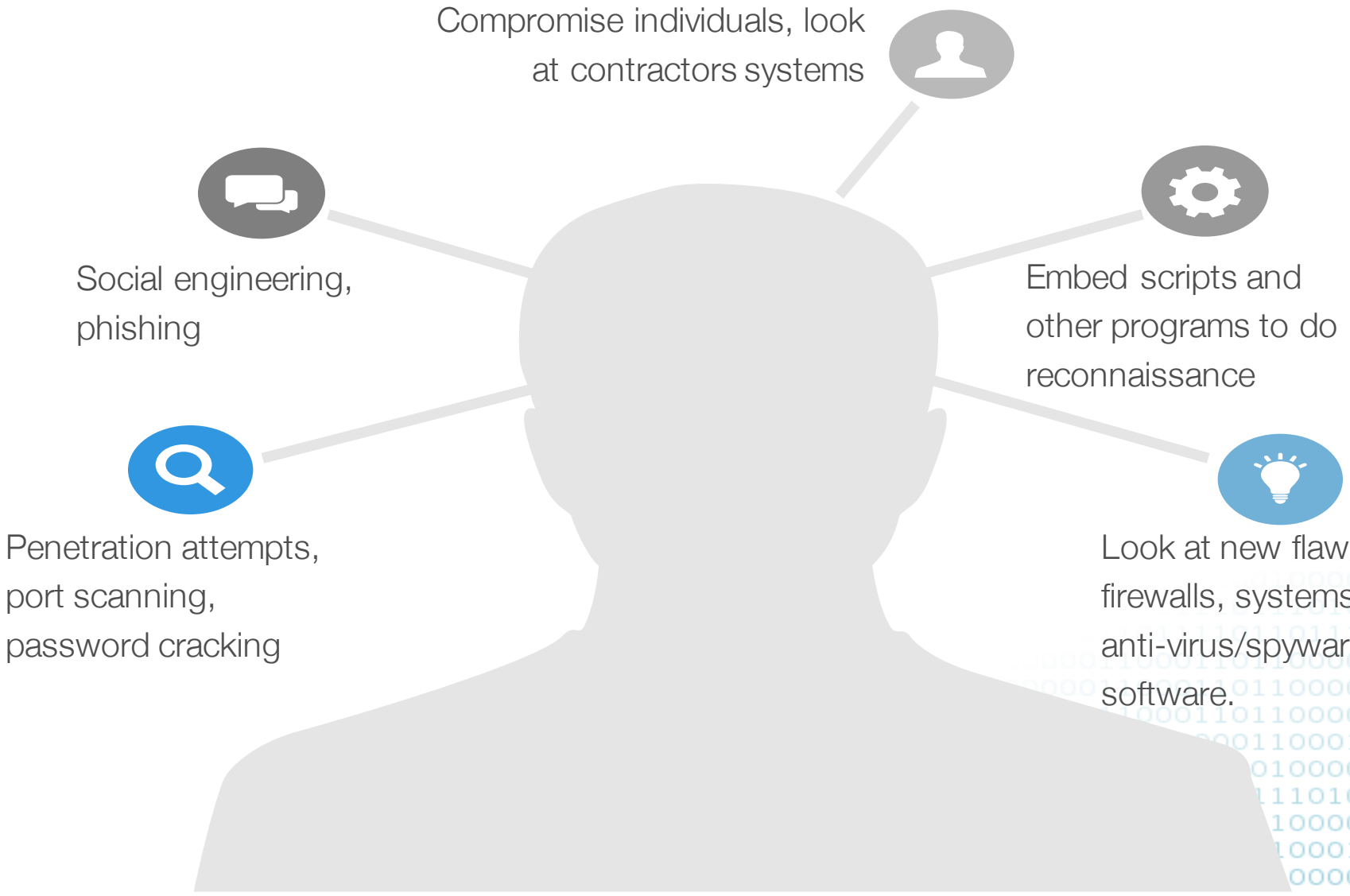
Step 1

Roadmap Step 1 - Assess Your Risk

- Not every organization is at risk from direct attack.
  - Understanding risk is key to how to build your roadmap to cyber security success.
  - Most are at risk for indirect attacks, BOTS, script-kiddies, etc.
  - Example: CryptoLocker is a nasty virus that many companies got caught by during that 200-day window from Microsoft and were forced to pay to have their files unlocked.

- Have serious discussions with your key stakeholders and try and identify risks. Put yourself in a hacker's shoes. What do they think?

What does a hacker think?



Compromise individuals, look at contractors systems

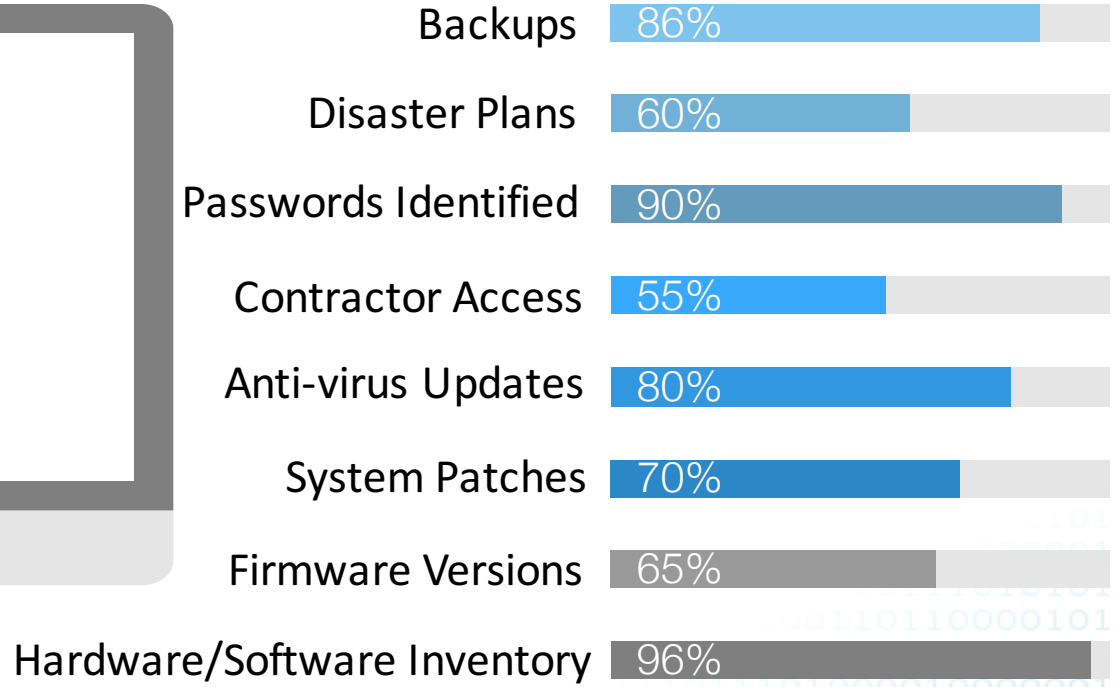
Social engineering, phishing

Embed scripts and other programs to do reconnaissance

Penetration attempts, port scanning, password cracking

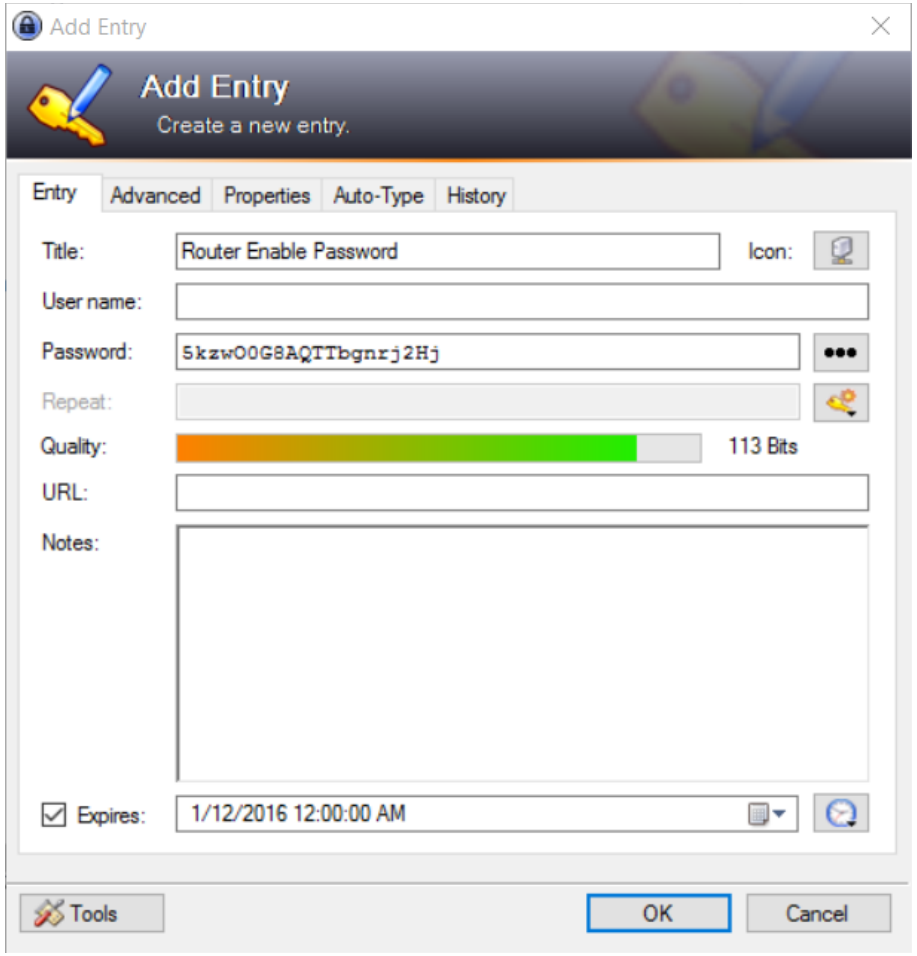
Look at new flaws in firewalls, systems, and anti-virus/spyware software.

Roadmap Step 2 - Evaluate Your Systems



Leave no stone unturned in your systems analysis. Hackers, BOTs, and script kiddies won't.

Secure Your Passwords



- There are many programs to help you create very secure passwords.

- We use KeePass which allows you to reveal the password or cut/paste. It gets rid of simple passwords like Password!

Roadmap Step 3 – PEN Testing

- Step 3 – PEN Testing
  - One of the best initial steps is to have a qualified organization do proactive whitehat hacking in which the good guys analyze your systems and try to find holes in your security plan.
- There are three steps to this:
  - 3.1 Test prep. In this step, do your best to find and fix what you can.
  - 3.2 Contract a PEN Testing company and execute a detailed SOW.
  - 3.3 Work to fix any vulnerabilities uncovered.

Plan Your Work and Work Your Plan

3.1 PEN Testing Prep

In a few weeks you should be able to understand how at risk you are and what gapping holes exist.

3.2 PEN Testing

Set realistic but aggressive goals for this. Just think, a script-kiddie might be on your system “right now” doing this.

3.3 Remediation

With your consultants, create an aggressive strategy to fix what is broken.

Roadmap Step 4 – Whitelist Software and Change Management

- Step 4 is crucial to your success.
  - 4.1 Install Whitelist software application
    - Remember our discussion on whitelist software? On your production system that is commissioned, unchanging, just running and making your widgets, your security team can map out:
      - Every executable that runs (DLLs, OCXs, COM Components)
      - Every network protocol, address, and port in use
      - Every network-aware application and who it talks to (system, address, protocol, port, target application)
      - Every user account

Roadmap Step 4 – Whitelist Software and Change Management (cont.)

- In blacklist software like Norton or McAfee, applications are able to run and your 200-day window to catch most attacks is in effect. Will your anti-virus really catch it?
- If you install whitelist software, first of all, all access accounts will be disabled. The hacker/BOT/script-kiddie will not even find anything for Admin to try and hack.
  - This is also impossible because the remote access ports are disabled!
  - For novelty, assume they get past this and they try to kick off a script/program; they would have to decrypt the whitelist database password which would inevitable involve trying to load more software.

    Everything is shutdown.

Roadmap Step 4 – Whitelist Software and Change Management (cont.)

- 4.2 Implement Change Management Software.
  - With Change-Management aware whitelist software, nothing can be done, altered, adjusted, unless an Approved CMR (Change Management Request) is completed.
  - This is total access control.
  - This is total protection.
  - It does not matter when or if your anti-virus software gets updated, and in fact, after a parallel installation for several months, we would encourage you to first disable, and eventually delete your blacklist software.
    - Why tax your production with software that consumes resources but doesn't really do its job?
  - This is true cyber "security".

Sounds Too Good To Be True

- What are the drawbacks, this sounds too good to be true?
  - Remember, we said you are never 100%. Part of your Security Analytics data is to be arm in arm with your whitelist software vendor. Their software will be under constant attack. Even so, the layers of access (ports, accounts, whitelist applications, etc.) make it very difficult to compromise.
  - Internal disgruntled employees can sabotage your system if they are on the ACL and can get your qualified managers to approve CMRs.
  - Education is key here. Blind CMR approvals are a no-no and having backups and disaster recovery plans in place are crucial to this internal attack.

Still Sounds Too Good To Be True

- One other drawback is the speed of access. It takes time to approve CMRs, it takes time to deal with the whitelist software.
  - If I have an emergency and have to deal with overriding CMRs it will hurt my production!
    - We will concede that this may be true, but with the use of mobile devices and easy CMR approvals this is an acceptable delay—we are talking minutes, not hours.

How do I start?

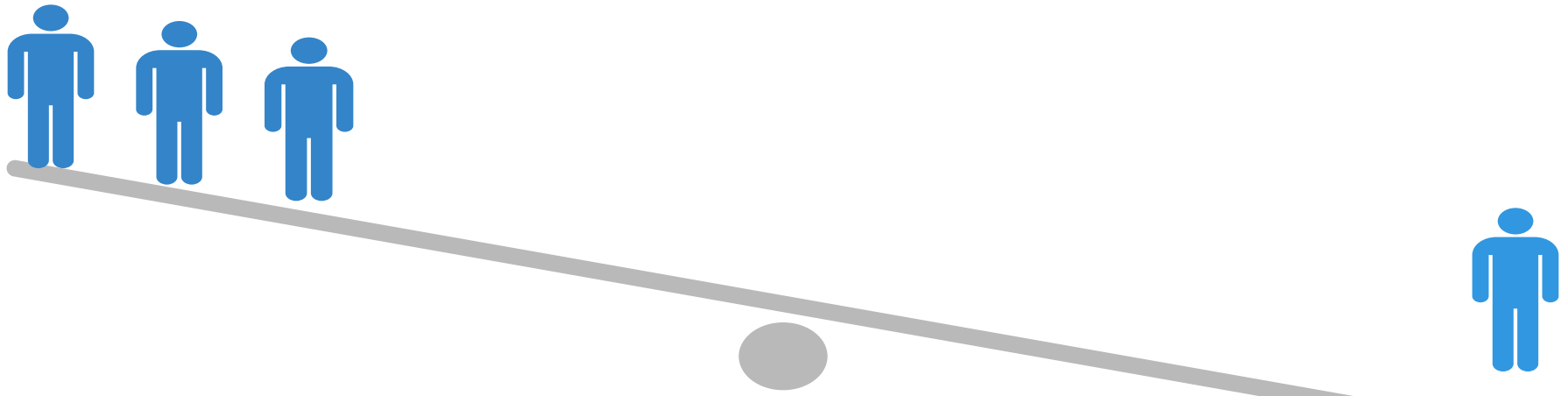
Hire An Expert Person/Firm

- A security expert is a specialized person in the field of cyber security.
  - How many of you have your system engineer or similar try doing their normal job…and…doing tasks for cyber security?
- They are up to date on breaches, constantly analyzing your systems, and are building a database of your business' security analytics (users, systems, ACLS, protocols, ports, software, outside connections, etc.).

Proactive Response

A breach hits the news and it affects WonderWare software. Your security professional can immediately put monitoring into place to assess risk in offices or plants that have the effected software.

Invest In Security Expert or Firm



One focused security expert is easily worth their weight in gold.

What are the ballpark costs?

Expect Cyber Security Costs to Rise with Factory Size

50 people	150 people	300 people	500 people
$60k	$162k	$324k	$540k

Estimate 60k for a 50 person factory and roughly 90% of that for every 50 persons. This is of course dependent on the number of systems, types of platforms, etc.

Summary

- There is always risk.
- Balancing risk with production needs can be difficult to map out, however, your efforts will not be wasted. It is not difficult, just detailed.
- Hackers are ahead of blacklist software vendors and you just cannot afford to be unprotected.
  - The statistics and research are undeniable. Just ask Google…Yahoo…
- Implementing Change Management and a whitelist software methodology can provide a cyber security model that does not wait to react—it is a proactive protection methodology that will keep your production secure.