

Cyber Security in a Nutshell

Verizon Data Breach Investigation Report 2016

Industry	Total	Small	Large	Unknown
Accommodation (72)	362	140	79	143
Administrative (56)	44	6	3	35
Agriculture (11)	4	1	0	3
Construction (23)	9	0	4	5
Educational (61)	254	16	29	209
Entertainment (71)	2,707	18	1	2,688
Finance (52)	1,368	29	131	1,208
Healthcare (62)	166	21	25	120
Information (51)	1,028	18	38	972
Management (55)	1	0	1	0
Manufacturing (31-33)	171	7	61	103
Mining (21)	11	1	7	3
Other Services (81)	17	5	3	9
Professional (54)	916	24	9	883
Public (92)	47,237	6	46,973	258
Real Estate (53)	11	3	4	4
Retail (44-45)	159	102	20	37
Trade (42)	15	3	7	5
Transportation (48-49)	31	1	6	24
Utilities (22)	24	0	3	21
Unknown	9,453	113	1	9,339
Total	64,199	521	47,408	16,270

Table 1.

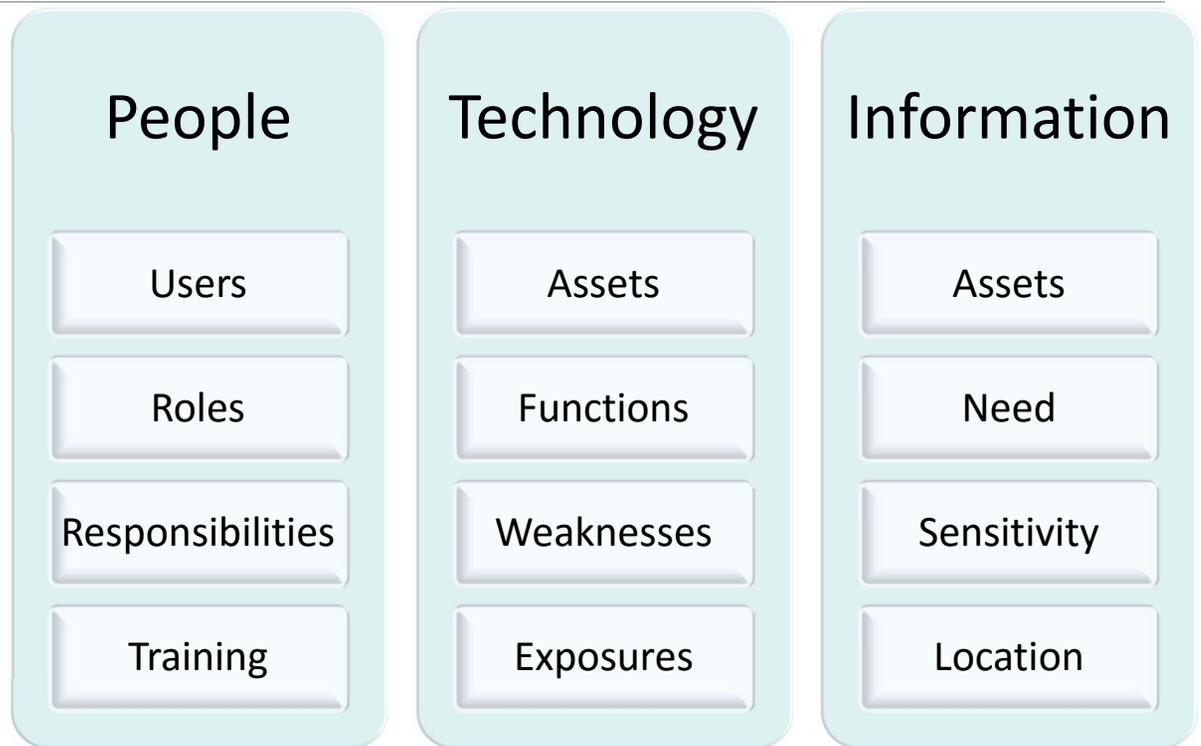
Number of security incidents by victim industry and organization size, 2015 dataset.

Industry	Total	Small	Large	Unknown
Accommodation (72)	282	136	10	136
Administrative (56)	18	6	2	10
Agriculture (11)	1	0	0	1
Construction (23)	4	0	1	3
Educational (61)	29	3	8	18
Entertainment (71)	38	18	1	19
Finance (52)	795	14	94	687
Healthcare (62)	115	18	20	77
Information (51)	194	12	12	170
Management (55)	0	0	0	0
Manufacturing (31-33)	37	5	11	21
Mining (21)	7	0	6	1
Other Services (81)	11	5	2	4
Professional (54)	53	10	4	39
Public (92)	193	4	122	67
Real Estate (53)	5	3	0	2
Retail (44-45)	137	96	12	29
Trade (42)	4	2	2	0
Transportation (48-49)	15	1	3	11
Utilities (22)	7	0	0	7
Unknown	270	109	0	161
Total	2,260	447	312	1501

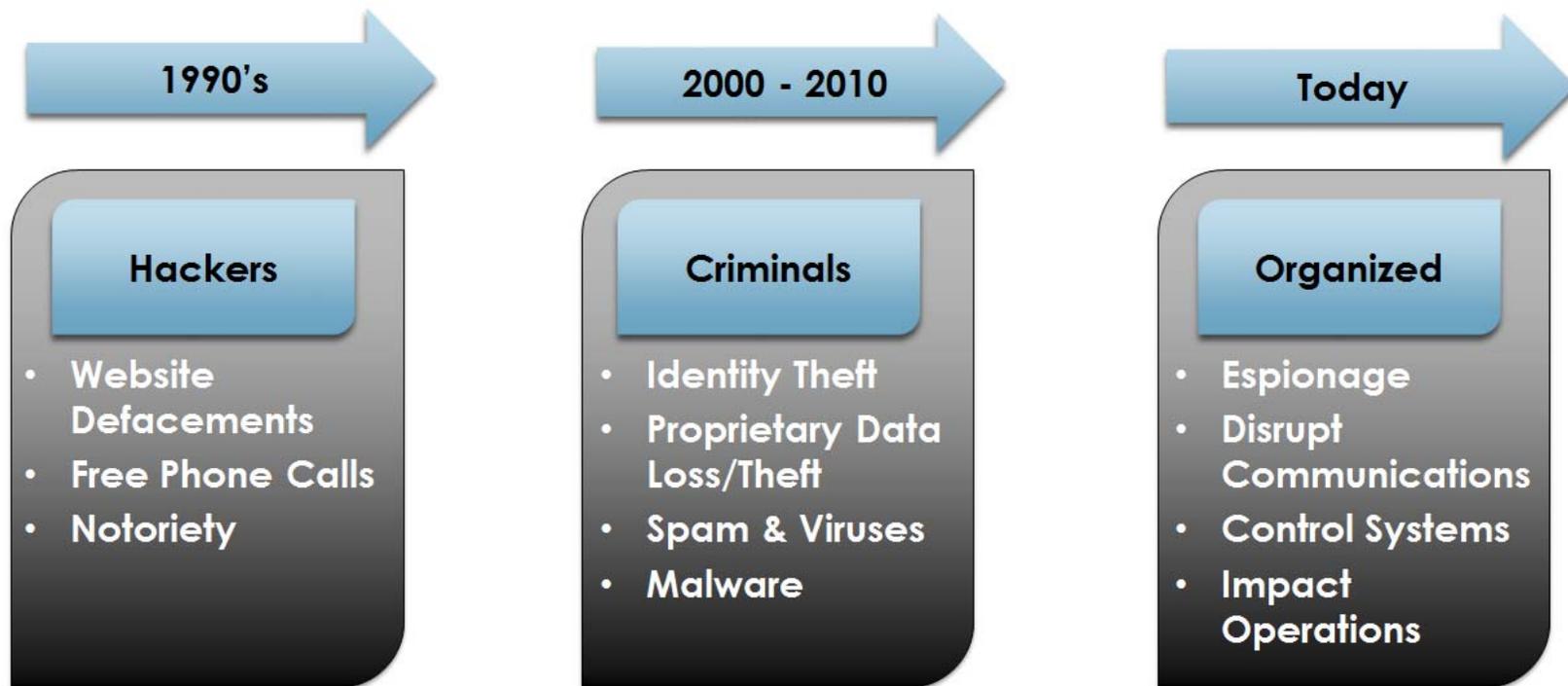
Table 2.

Number of security incidents with confirmed data loss by victim industry and organization size, 2015 dataset.

What is Cyber Security?



What is the history of Cyber Crime?



Who are the Cyber Criminals?



What do Cyber Criminals want?

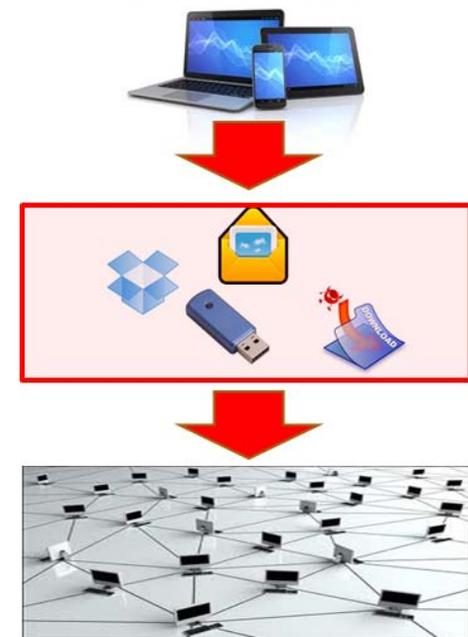


How do they get what they want?

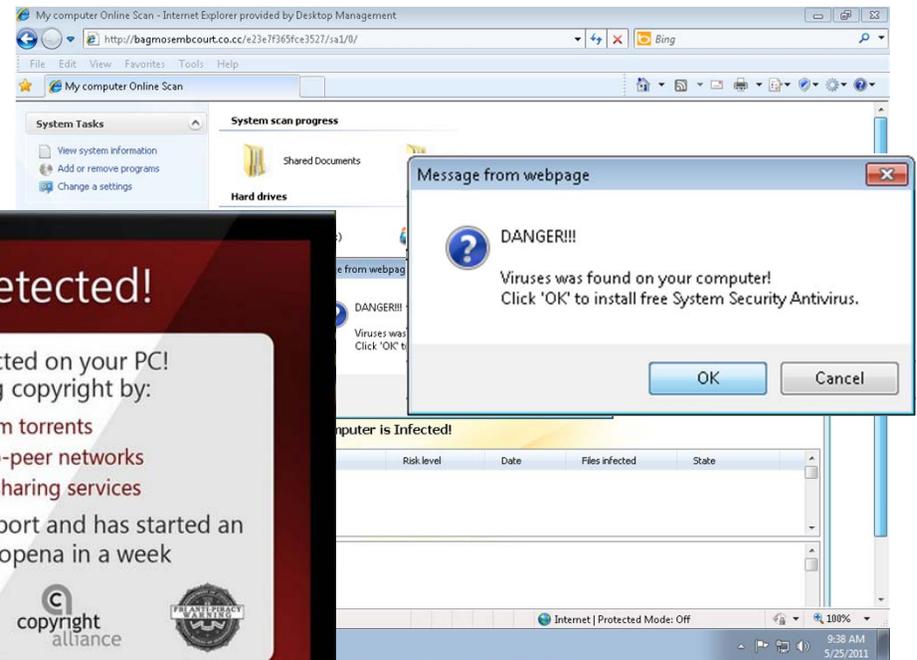


What is Malware?

Malware Name	Description
InfoStealer.Banker.Zbot	Focuses on stealing sensitive online banking information e.g. credit card number, pin code and passwords
Trojan.Asprox	Trojan.Asprox is a Trojan horse that uses the compromised computer as a proxy server.
Trojan.Sisron	Program that grants unauthorized access to a computer, often through a backdoor.
Trojan.ZeroAccess	Trojan horse that uses an advanced rootkit to hide itself. It can also create a hidden file system, downloads more malware, and opens a back door on the compromised computer



Notable Malware “RansomeWare”

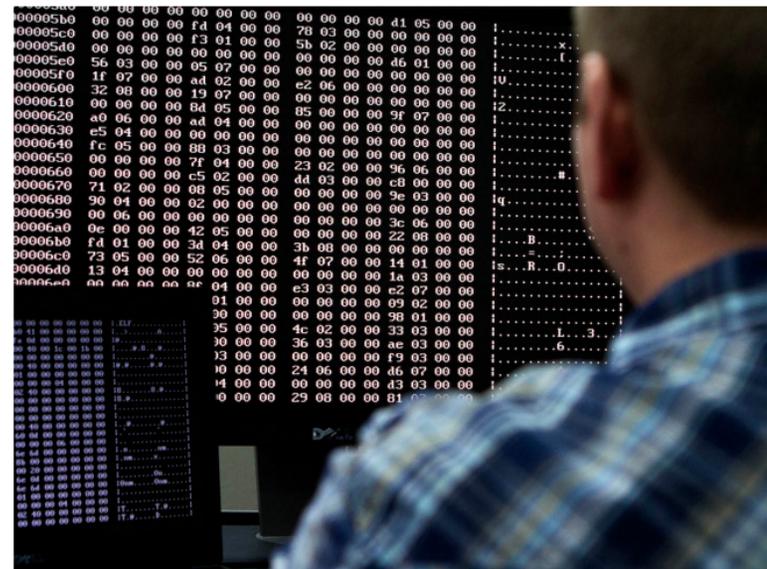


The Cost of Ransomware

Victims paid more than \$24 million to ransomware criminals in 2015 — and that's just the beginning

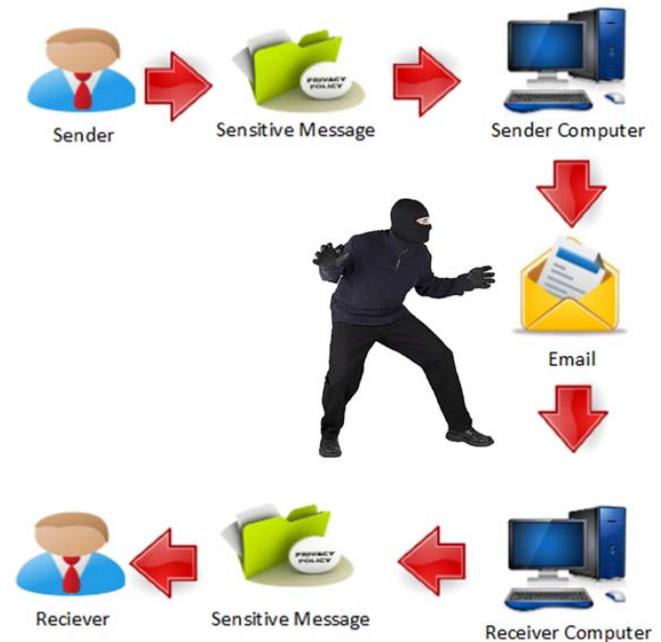
BUSINESS INSIDER By Dan Turkel

Fri, Apr 8, 2016, 5:26pm EDT



The Real Danger

63% of confirmed data breaches involved weak, default or stolen passwords.



Password Security

Open Sesame

Most popular passwords of the past 4 years

	2011	2012	2013	2014
1	password	password	123456	123456
2	123456	123456	password	password
3	12345678	12345678	12345678	12345
4	qwerty	abc123	qwerty	12345678
5	abc123	qwerty	abc123	qwerty
6	monkey	monkey	123456789	123456789
7	1234567	letmein	111111	1234
8	letmein	dragon	1234567	baseball
9	trustno1	111111	iloveyou	dragon
10	dragon	baseball	adobe123	football

Source: SplashData

The Wall Street Journal

number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years

Protecting your username and password

Change initial, reset or default passwords when you first log on

Use different passwords for different accounts

Create unique passwords that do not contain personal information and are not common

Ensure the password has at least 8 characters with a combination of upper and lower case letters and a number

Do not share passwords

Do not use post it notes or open lists for passwords

Good Password Techniques



DarthKitten&LukeWhitewh1sker



DogeSaystofollowURdreams

LoveDrivingmy19fourtyFord



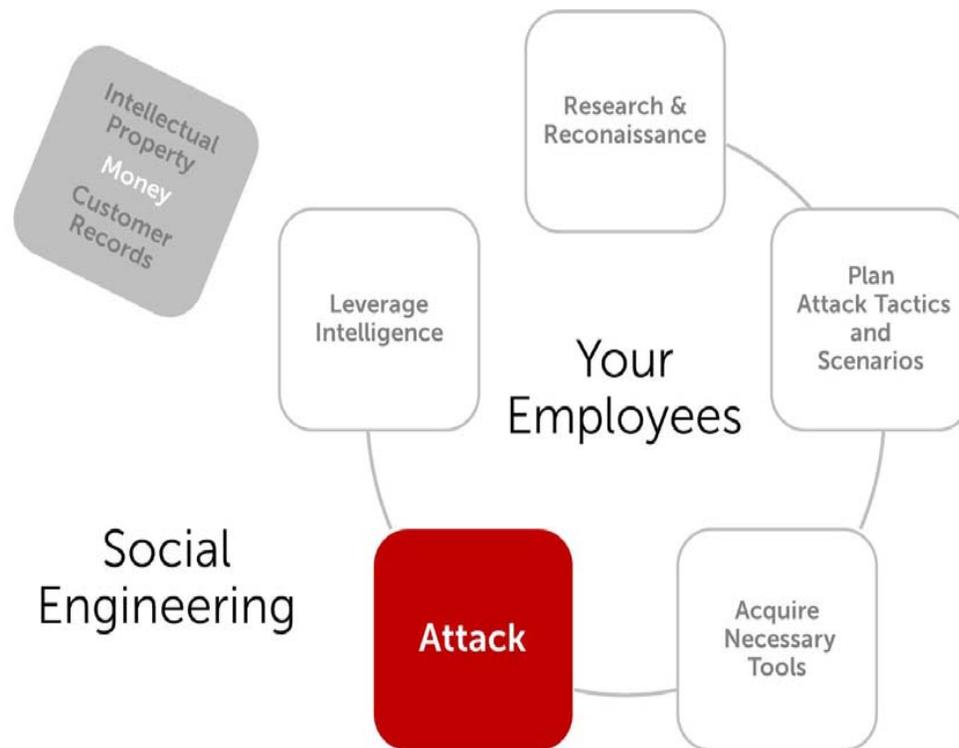
Social Media Risk Mitigation

The image shows a screenshot of a Facebook profile for Angela Kay Echols. Several red callout boxes with arrows point to specific pieces of information on the profile:

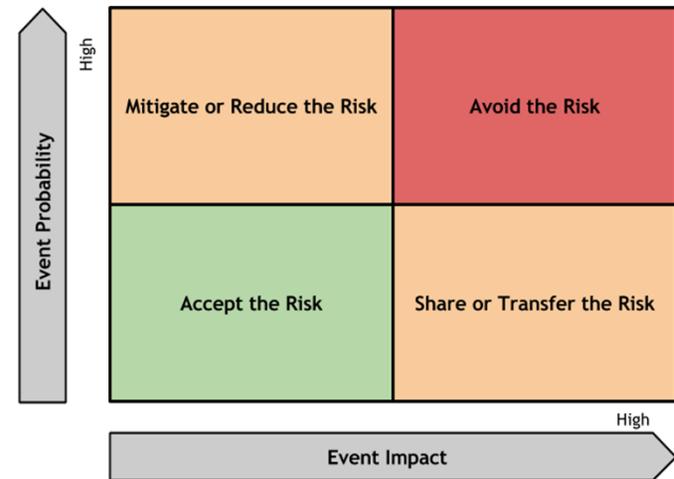
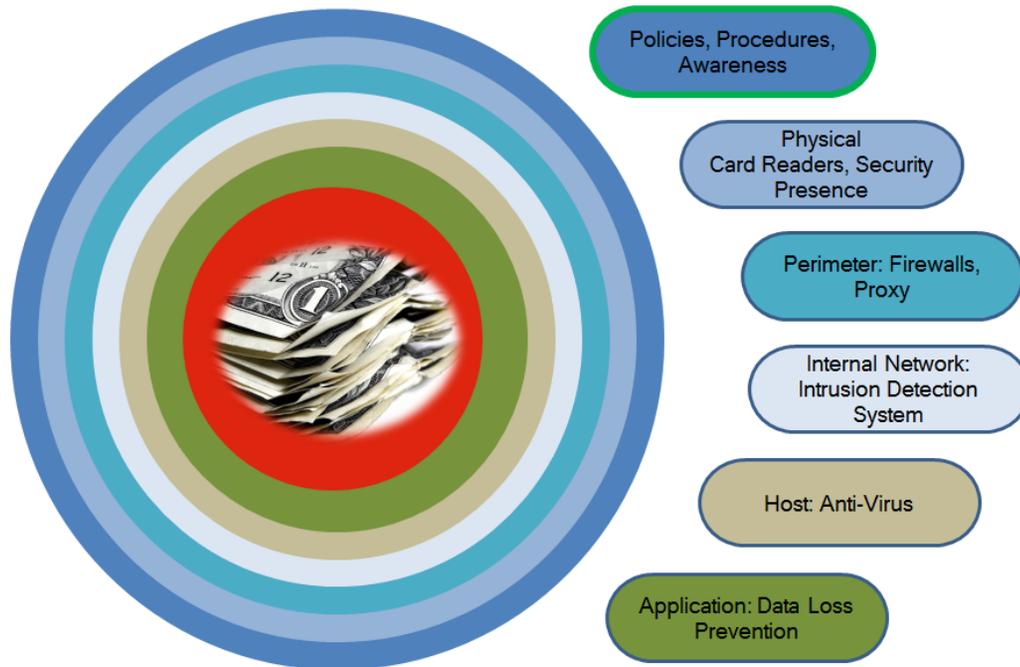
- Place of Birth:** Points to the 'Living' section, specifically to 'Phoenix, Arizona' and 'Colorado Springs, Colorado'.
- Mothers Maiden Name:** Points to the 'Family' section, specifically to 'Trish Tomines'.
- Details about you:** Points to the 'Basic Information' section, specifically to 'September 11', 'Female', 'Married to Michael Echols', and 'April 12, 2003'.
- Contact Information:** Points to the 'Contact Information' section, specifically to '(602) 471-2095' and 'angela.k.echols@facebook.com'.

The profile also displays work and education history, including 'U.S. Department of Veterans Affairs' and 'Boulder County Department of Social Services'. The right sidebar shows a list of friends and recent activity.

Social Media Risk Mitigation



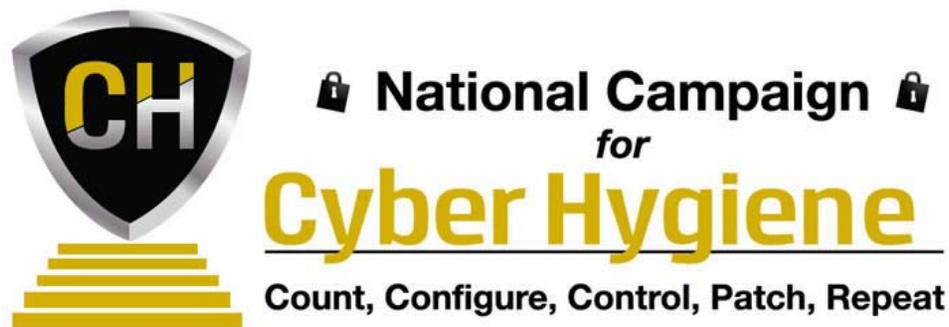
Defense in Depth



More than Firewalls and Anti-Virus



National Programs (MS-ISAC)



<https://www.cisecurity.org/cyber-pledge/>

Count	Cyber Hygiene Priority - COUNT: Know what's connected to your network
Configure	Cyber Hygiene Priority - CONFIGURE: Protecting your systems by implementing key security settings.
Control	Cyber Hygiene Priority - CONTROL: Protecting your systems by properly managing accounts and limiting user and administrator privileges to only what they need to do their job.
Patch	Cyber Hygiene Priority - PATCH: Protecting your systems by keeping current!
Repeat	Cyber Hygiene Priority - REPEAT: Protecting your systems by keeping current!

Questions



Michael Echols, CISSP

- Chief Information Security Officer, Maricopa County, AZ
- Cyber Security Adjunct Faculty, Estrella Mountain Community College, Avondale, AZ
- Author “Smart Grid Security: An End-to-End View of Security in the New Electrical Grid”

