SAME Presentation on Cybersecurity

Andy Knauf CIO – Mead & Hunt

Mead&Hunt

EMPLOYEE-OWNED ENGINEERING & ARCHITECTURE FIRM

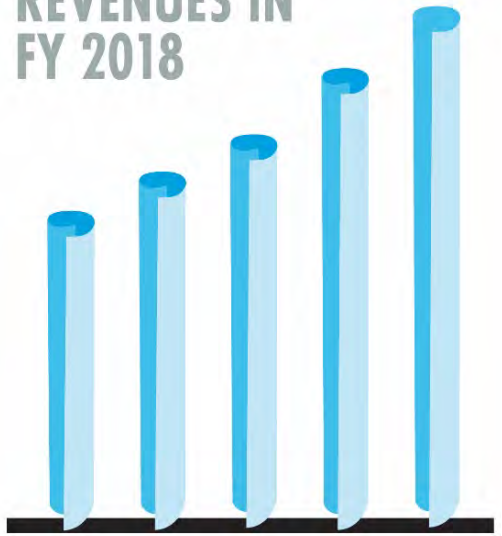
~900 EMPLOYEES

ENGINEERS • ARCHITECTS • SCIENTISTS • PLANNERS

ONE OF THE BEST PLACES TO WORK BY CE NEWS

#119 TOP 500 DESIGN FIRM BY ENGINEERING NEWS RECORD

$137 MILLION REVENUES IN FY 2018




OUR DEVICES ARE NOW 100% SECURE.
I TURNED THEM ALL OFF.
HOW DID YOU DO THAT?
© D.Fletcher for CloudTweaks.com

Focus on the basics

Regular patching is essential as criminals exploit known vulnerabilities.

Cyber Security awareness training, two factor authentication and good password management strategy need to be considered carefully.

IT Security Review

A good IT organization will conduct a review of the present systems & network to assess the protection level, identify gaps and recommend solutions to limit future risk.

INTERNET SECURITY TESTING

The engineers will scan Internet-visible hosts, identify services running on the hosts, and conduct testing for vulnerabilities to known exploits. Test results will be manually validated, as necessary, in an effort to minimize false-positive reporting. Where appropriate, the engineers may exploit vulnerabilities in order to more accurately determine the risk to your environment.

Penetration Testing – Penetration testing of key organizational IT assets will be performed, in an attempt to gain access to these key assets and provide documentation on the path to access.

Domain Security and Password Audit – An audit of passwords and password-related policies used within the organization will be performed, with guidance provided on potential improvements. This item is limited to a single Active Directory domain.

Authenticated Scan – Up to 50 workstations will be tested via an authenticated scan. The results of this scan, once validated, should provide a good snapshot of workstation security.

WIRELESS SECURITY TESTING

The engineers will scan the 802.11-based signal cloud around your network testing for ways that outsiders could eavesdrop on your wireless communications, break authentication or cryptographic protocols, or impersonate elements of your wireless infrastructure. The Wireless Test portion of the offering is limited to one physical site.

SOCIAL ENGINEERING PHISHING EXERCISE

Social Engineering is a process in which access is gained to a network using People, Process often combined with technology. Various types of social engineering can be used by a hostile party to exploit a network. We will only demonstrate non-malicious and non-harmful Social Engineering Techniques to demonstrate these possible vulnerabilities. We propose a Phishing Attack against the employees (computer users) of the customer network.

Social Engineering & Phishing exploit against the users of users of the customer network.

Email addresses can be mined from the Internet or the customer can provide list of the user email addresses.

Layered approach

There is no one stop solution when it comes to good cyber security measures.

The key is layering – antivirus is one layer, others are next gen firewalls, secure offsite repository and disaster recovery.

Handset Management

One of the biggest risks facing businesses today is the dramatic increase in mobile devices that are accessing their network.

They pose a serious security risk if not properly protected and managed.

Ongoing Monitoring

Identifying threats before they cause any damage is the mainstay of preventing a security threat from taking hold.

Monitoring activity on an ongoing basis can help mitigate this risk.

Questionnaire Reference No.	A. Security Policy	Yes / No	NIST 800-53R4 Control Number	NIST 800-53 Control Name
SP-3	Is there an information security policy that addresses the confidentiality, integrity, and availability of computing resources and information assets that has been approved by your senior management?	Yes	CA-1 AC-1 AT-1 AU-1 IA-1 IR-1 MA-1 PE-1 PL-1 PS-1 RA-1 SA-1 SC-1 SI-1 CM-1 CP-1	Security Assessment and Authorization Policies and Procedures Access Control Policy and Procedures Security Awareness and Training Policy and Procedures Audit and Accountability Policy and Procedures Identification and Authentication Policy and Procedures Incident Response Policy and Procedures System Maintenance Policy and Procedures Media Protection Policy and Procedures Physical and Environmental Protection Policy and Procedures Security Planning Policy and Procedures Personnel Security Policy and Procedures Risk Assessment Policy and Procedures System and Services Acquisition Policy and Procedures System and Communications Protection Policy and Procedures System and Information Integrity Policy and Procedures Information Security Program Plan
	B. Risk Assessment and Treatment			
RAT-1	Is a program in place to monitor identified cybersecurity risks and determine the effectiveness of compensating	Yes	RA-1	Risk Assessment Policy and Procedures
RAT-2	Has an identification and analysis of likely cyber threats been completed?	Yes	RA-3	Risk Assessment
RAT-5	Is there a third party vendor management program in place?	Yes	SA-12	Supply Chain Protections
RAT-6	Do you conduct oversight of your third party service providers including those who help process or host PG&E provided data on your behalf (e.g. vendors, consultants,	Yes	SA-12	Supply Chain Protections
RAT-7	Is cyber security due diligence performed on third party service providers prior to entering into a business relationship with them? If so, please provide a sample of	No	SA-12	Supply Chain Protections
RAT-8	Do you include information security requirements in contracts with your third party service providers? If yes, please provide sample contractual language.	No	SA-12	Supply Chain Protections
	D. Asset Management			
AM-1	Are your information assets classified? If yes, please describe your classification scheme in the comments.	No	RA-2	Security Categorization
AM-2	Do you protect data based upon the classification (e.g. PII, restricted)?	No	MP-2 MP-3 MP-4 MP-5 MP-6 MP-7 PE-20 SC-8 SC-28	Media Access Media Marking Media Storage Media Transport Media Sanitization Media Use Transmission Confidentiality and Integrity Protection of Information at Rest

Every second 12 people online become a victim of cybercrime.
3500 people devoted to Cyber Security at Microsoft.
Network Assessment
Security Assessment
Social Engineering Phishing Engagement
Multi-Factor Authentication\Increased complexed passwords\unique phrases
Training (KnowBe4, Mimecast)
Backup plans
Windows 10 and Patch Management
Data sharing with other companies

Questions