



The Zen Ten Cyber Security Protection for Oregon Cities

Greg Hardin, Cybersecurity Specialist/Systems Architect
Scott Moss, Program Administrator

CIS

Objectives

- Highlight examples from claims experience
- Explain the Zen Ten Cyber Security Protections
- Coverage tiers, premium, and limits
- Claims process



Cyber Threats Close to Home

Three claims prior to 2018

47 claims since 2018

Cyber attacks are up 600%
worldwide since the start of
pandemic



Ransomware



Coastal county with nearly 500K incurred costs

Two small cities over 100K

Fraudulent Instruction

- City paid bad actor posing as contractor
- Bad actor stole email credentials of contractor



Release of PII



- County paid nearly 80K for notifications
- Bad actor gained access to email for 10 hours

Introduction

Greg Hardin
Cybersecurity Specialist/
Systems Architect
503-763-3889
ghardin@cisoregon.org



How do I
protect my
entity against
cyber risk?

ZEN TEN



Do you have policies related to cybersecurity?

Yes

No

1) Adopt a cybersecurity policy

2) MFA (Multi-Factor Authentication)



3) EDR/XDR

- SentinelOne
- Cortex XDR
- Windows Defender ATP
- Carbon Black
- CrowdStrike
- Darktrace
- Albert Sensors (MS-ISAC)



4) Immutable Geo-diverse backups

Backups should be:

- Gated
- Offline
- In a different Geo region
- Tested on a random, monthly, quarterly, and annual basis



5) Training

CIS' learning center offers online cyber security awareness training



Cyber Security: Phishing Prevention
Course (1 class)
Phishing is one of the most dangerous and common cyber security risks today. This module takes a close look at the different types of phishing and provides tips to help you avoid being caught out. Objectives: Learn about the different types of phishing ...more
★★★★★ LAUNCH

Cyber Security Basics
SUCCESSFUL
Course (1 class)
This course will help you identify potential cyber threats, including malware, phishing and session hijacking, and take important steps to protect your company's valuable information. Cyber-crime syndicates, along with the prevalence of mobile and cloud-b ...more
View credits
★★★★★ PRINT CERTIFICATE

Understanding Cyber Security
Course (1 class)
Advances in technology have changed the way we live and the way we do business. Our world is more connected than ever before. This brings huge opportunities and benefits, but it also brings risks. This course can help to understand these risks. Objectives ...more
★★★★★ LAUNCH

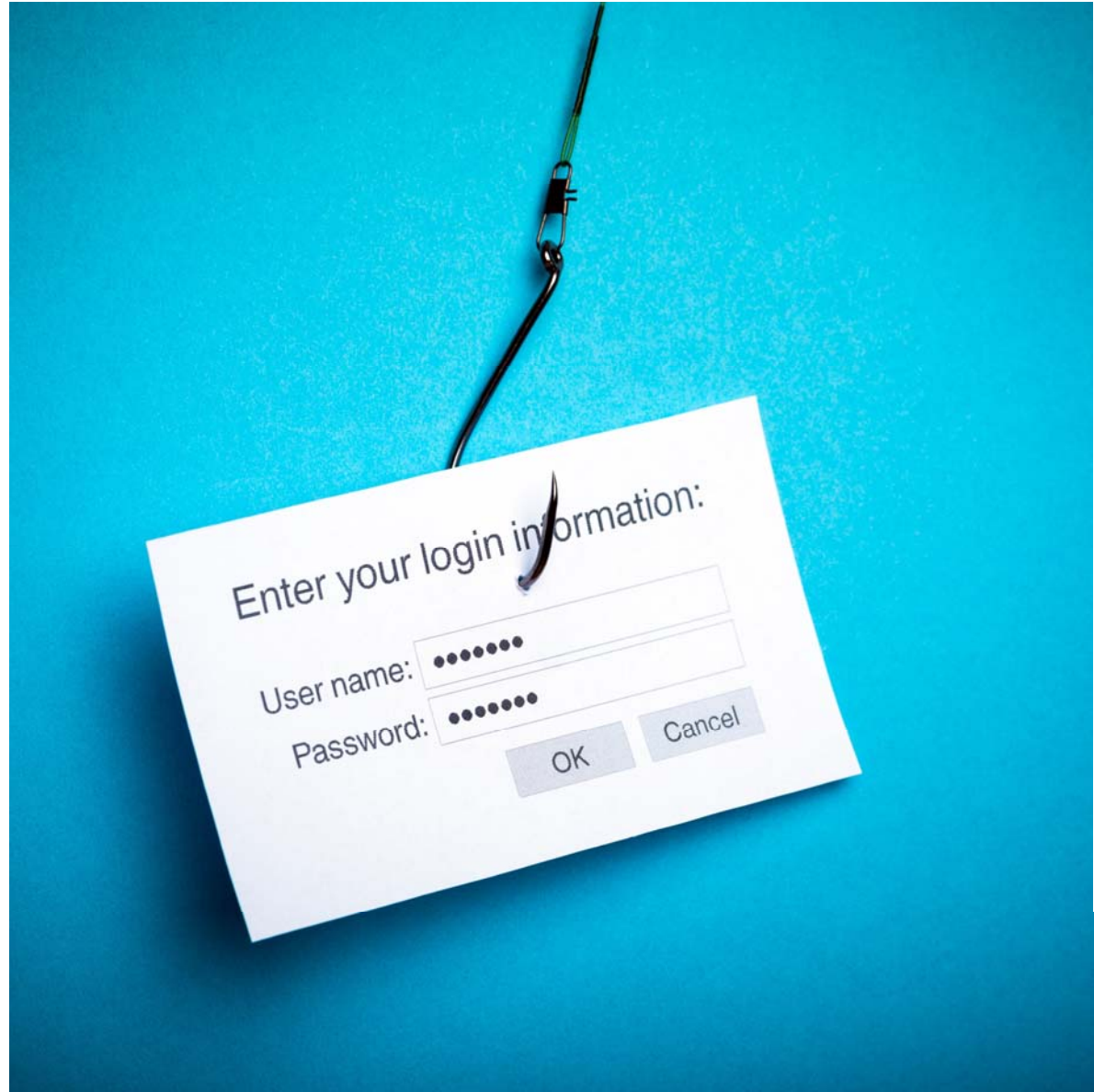
Cyber Security for the End User
Course (1 class)
Became estimates, over 90% of security breaches are ...more
★★★★★ LAUNCH

Cyber Security Essentials: Stop. Think. Ask.™
Course (1 class)
Cybersecurity is the practice of protecting systems ...more
★★★★★ LAUNCH

Cyber Security: Risks and Social Media (Global)
Course (1 class)
This course discusses how social media affects you and ...more
★★★★★ LAUNCH

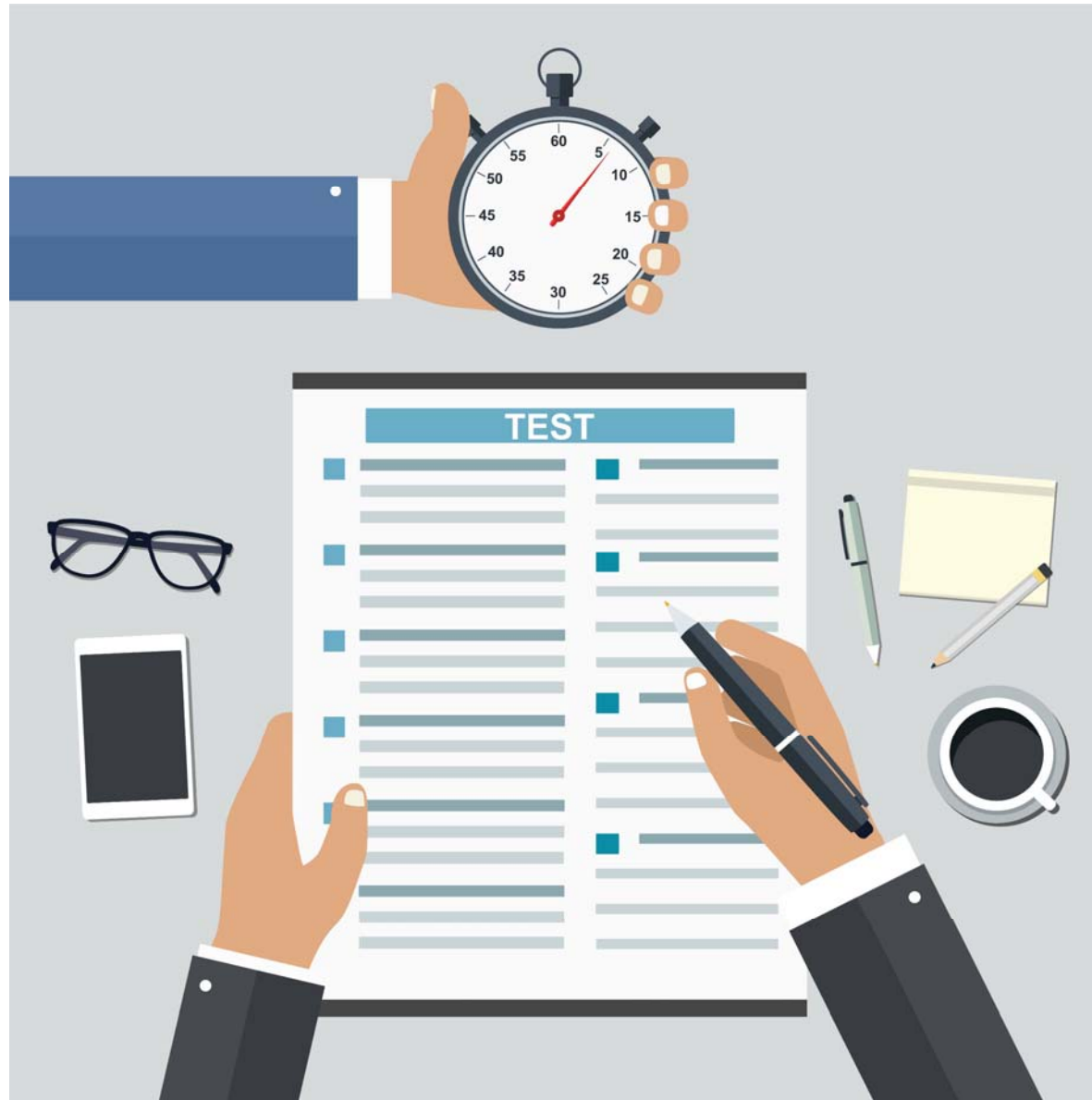
6) Phishing exercises or social engineering tests

88% of data breaches come from human error



Tips for acing the test

- Use a different communication channel to verify the request
- Be suspicious of urgent requests asking for immediate action
- Inspect the from email address and the reply to address
- Hover over links to confirm they match the expected primary domain.
- Know your company policy on password change requests



Vulnerability Scanning



**CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY**



Cyber Hygiene Scan

Web Application Scan

Email: Therese Masse
theresa.masse@cisa.dhs.gov



Verify your password's uniqueness


Use haveibeenpwned.com to check if your email or phone number has been compromised

Use haveibeenpwned.com/passwords to check if your password is unique across all known data breaches



123456 has been pwned over 24 million times

A screenshot of a password checker interface. At the top, a search bar contains the password '123456' and a 'pwned?' button with a magnifying glass icon. Below the search bar, a dark red banner displays the message: 'Oh no — pwned! This password has been seen 24,230,577 times before. This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!'

123456  pwned?

Oh no — pwned!
This password has been seen 24,230,577 times before
This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!

7) Require complex passwords

- Longer passwords, not frequent expiration
- Use a password manager
- All password managers will generate one for you



Email Filters

Add custom message identifying outside emails



8) Patches

Stay updated on patches



9) User Auditing



Do you limit the number of administrative users?

Do you audit systems for users that may have access that no longer need it?

Add an expiration date for IT when asking for contractor access

10) Purchase cyber insurance coverage (from CIS)



Coverage Tier Limits

CIS AGGREGATE:	\$5,000,000	\$5,000,000	\$5,000,000	\$5,000,000
TIER 1	\$50,000	\$50,000	\$50,000	\$50,000
TIER 2	\$200,000	\$200,000	\$200,000	\$200,000
<i>TIER 3</i>	<i>\$250,000</i>	<i>\$500,000</i>	<i>\$750,000</i>	<i>\$1,000,000</i>
TOTAL	\$500,000	\$750,000	\$1,000,000	\$1,250,000
Cyber Extortion Loss (Ransomware)	\$500,000	\$750,000	\$1,000,000	\$1,250,000
Data Recovery Costs	\$500,000	\$750,000	\$1,000,000	\$1,250,000
Reputational Loss	\$500,000	\$750,000	\$1,000,000	\$1,250,000
Data & Network Liability	\$500,000	\$750,000	\$1,000,000	\$1,250,000
Regulatory Defense & Penalties	\$500,000	\$750,000	\$1,000,000	\$1,250,000
Fraudulent Instruction	\$500,000	\$500,000	\$500,000	\$500,000
Funds Transfer Fraud	\$500,000	\$500,000	\$500,000	\$500,000
Telephone Fraud	\$500,000	\$500,000	\$500,000	\$500,000
Breach Response	\$500,000	\$750,000	\$1,000,000	\$1,250,000
Deductible	\$5,000	\$5,000	\$5,000	\$5,000



Tier 1 and 2 Premium

Materials & Services Budget	\$50k Limit (Tier One)	\$200k Limit (Tier Two)
\$0 - \$500K	\$650	\$500
\$500K - \$1M	\$800	\$650
\$1M - \$2M	\$1,200	\$850
\$2M - \$5M	\$2,300	\$1,100
\$5M - \$15M	\$3,600	\$1,500
\$15M - \$30M	\$5,500	\$2,100
\$30M+	\$7,500	\$3,000



Tier 3 Premium

TIER 3 PREMIUM				
<i>TIER 3</i>	\$250,000	\$500,000	\$750,000	\$1,000,000
POPULATION				
Under 9,999	\$1,500	\$2,800	\$4,200	\$5,500
10,000-24,999	\$2,200	\$5,500	\$6,900	\$9,500
25,000-49,999	\$3,500	\$8,200	\$10,200	\$13,600
50,000-99,999	\$5,500	\$11,000	\$13,700	\$20,500
100,000 plus	\$9,500	\$16,300	\$17,000	\$34,000



What Happens When A Claim is Filed

Call Carol!

1. Carol contacts "breach coach"
2. Meeting with you, IT, Carol, breach coach
3. Breach coach will tell you to call law enforcement
3. Forensics firm recommended – you get to decide and contract
4. Negotiation firm recommended (if needed)
You get to decide and contract

CIS Cyber Adjuster



Carol Drouet
Senior Property Claims
Consultant
503-763-3872
cdrouet@cisoregon.org



Detection and Remediation

How should the infected machines be handled?



Contact Information

Greg Hardin
Cybersecurity Specialist/
Systems Architect
503-763-3889
ghardin@cisoregon.org



Contact Info

Greg Hardin
Cybersecurity Specialist/
Systems Architect
503-763-3889
ghardin@cisoregon.org



Resources

- <https://cisoregon.org/Member/RiskManagement/ResourceLibrary>
- <https://learn.cisoregon.org/>
- <https://www.cisa.gov/>
- <https://www.cisecurity.org/ms-isac>



Insight – CIS Risk Management Software

Insight Templates

- *Cyber Detection*
- *Cyber Identification*
- *Cyber Protection*
- *Cyber Response and Recovery*
- *Cyber – Implementing MFA*

*Contact Scott Moss for more information
smoss@cisoregon.org*

