



The Evolution of Cyber Coverage at CIS

Greg Hardin, Cybersecurity Specialist/Systems Architect



CIS

Objectives

1. Brief history of cyber coverage at CIS
2. Highlight examples from claims experience
3. Define cyber coverage terms
4. Coverage tiers and limits
5. Identify minimal cyber hygiene to qualify for coverage
6. How can you help?

Introduction

Greg Hardin

Cybersecurity Specialist/
Systems Architect

503-763-3889

ghardin@cisoregon.org



About CIS

CIS (CityCounty Insurance Services) - cisoregon.org

- Formed in 1981 by the League of Oregon Cities and the Association of Oregon Counties
- Administers CIS Trust for members
 - 98% of cities
 - Over 78% of counties in Oregon
- Board consists of membership appointed by LOC and AOC

Why is cybersecurity so important?



“Every company is a software company”

**Richard Campbell
Podcaster and Microsoft MVP**



Cyber Threats are Escalating



Claims prior to 2018-2019: **1**



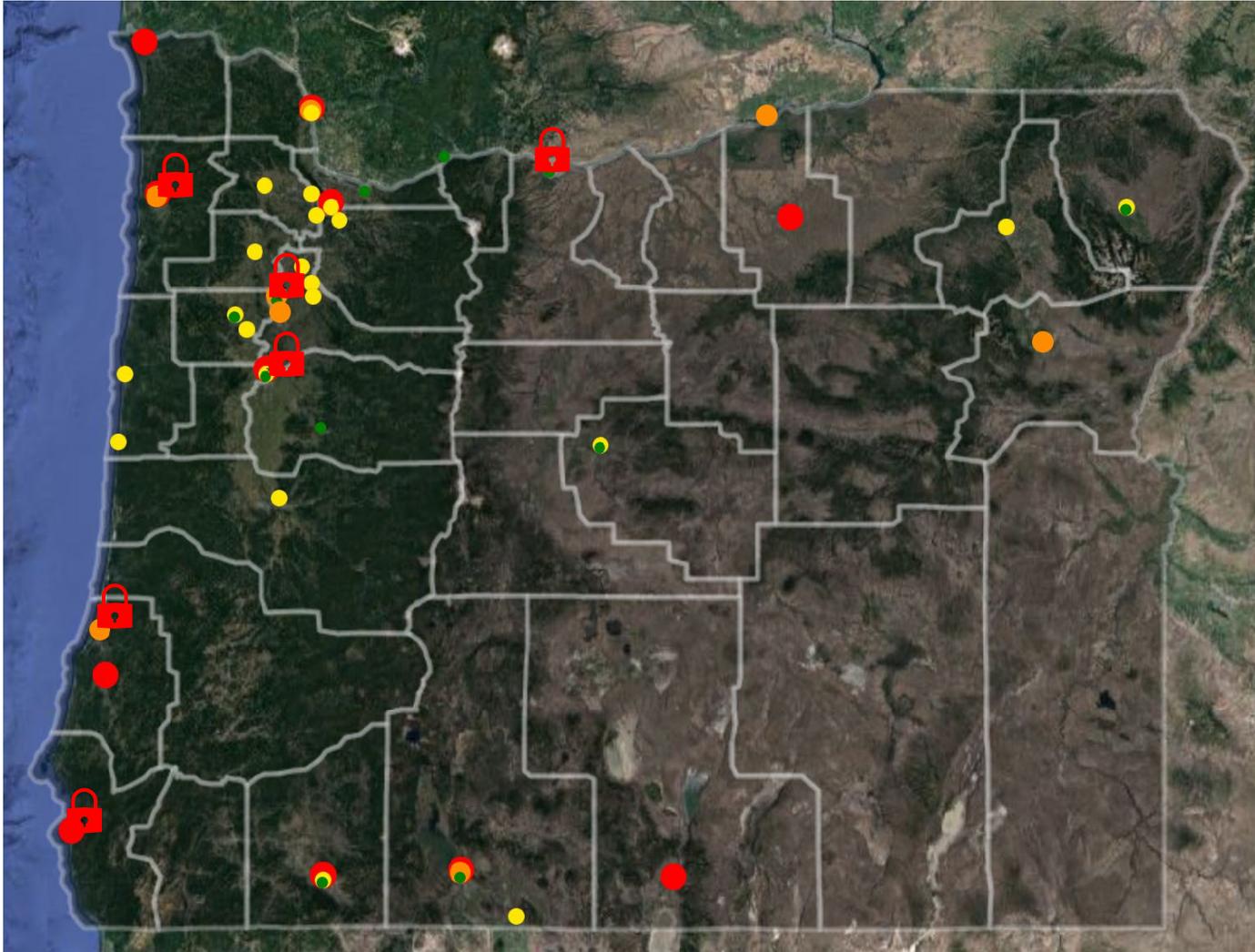
Claims since 2019: **54**



Cyber-attacks are up **600%** worldwide since 2020!



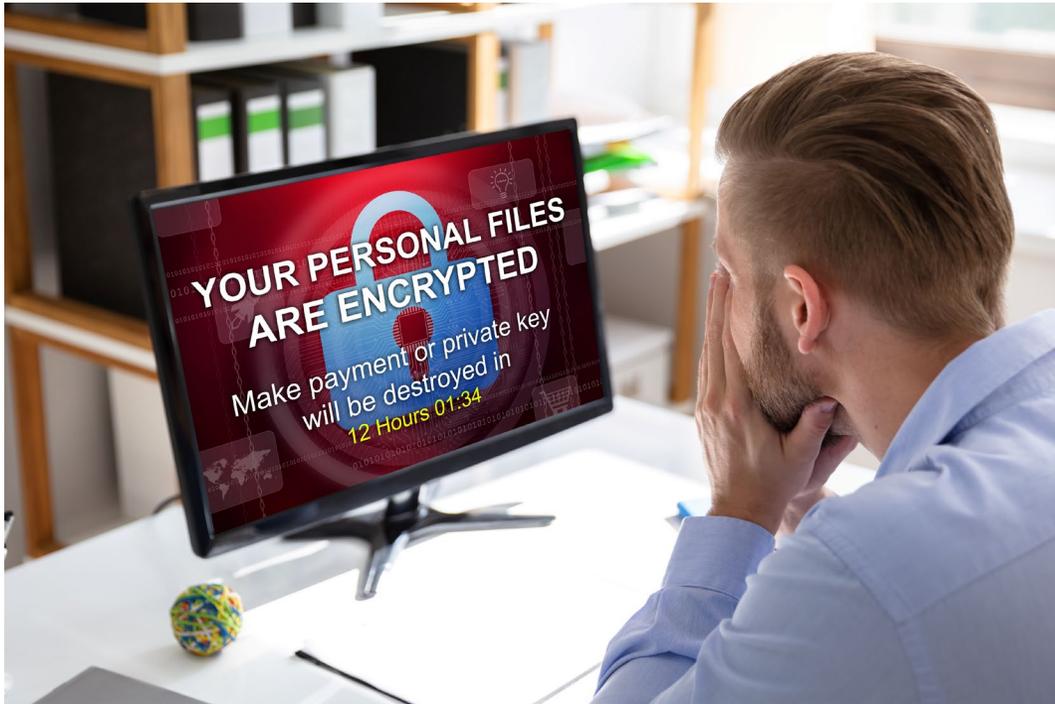
City and County Cyber Claims



 = Ransomware

- Red: Total incurred \geq \$50K
- Orange: Total incurred \geq \$25K and $<$ \$50K
- Yellow: Total incurred $>$ \$0 and $<$ \$25K
- Green: Total incurred = \$0

Ransomware



Coastal county with nearly 500K incurred costs

Two small cities over 100K

Recently, two coastal counties hit in the same week with Royal ransomware

Royal Ransomware Note

Hello!

If you are reading this, it means that your system were hit by Royal ransomware.

Please contact us via :

[http\[:\]//royal2xthig3ou5hd7zsliqagy6yygk2cdelaxtni2fyad6dpmxededid\[.\]onion/](http[:]//royal2xthig3ou5hd7zsliqagy6yygk2cdelaxtni2fyad6dpmxededid[.]onion/)

In the meantime, let us explain this case. It may seem complicated, but it is not!

Most likely what happened was that you decided to save some money on your security infrastructure.

Alas, as a result your critical data was not only encrypted but also copied from your systems on a secure server.

From there it can be published online. Then anyone on the internet from darknet criminals, ACLU journalists,

Chinese government (different names for the same thing),

and even your employees will be able to see your internal documentation:

personal data, HR reviews, internal lawsuits and complains, financial reports, accounting, intellectual property, and more!

Fortunately we got you covered!

Royal offers you a unique deal. For a modest royalty (got it; got it ?) for our pentesting services we will not only provide you with an amazing risk mitigation service, covering you from reputational, legal, financial, regulatory, and insurance risks, but will also provide you with a security review for your systems.

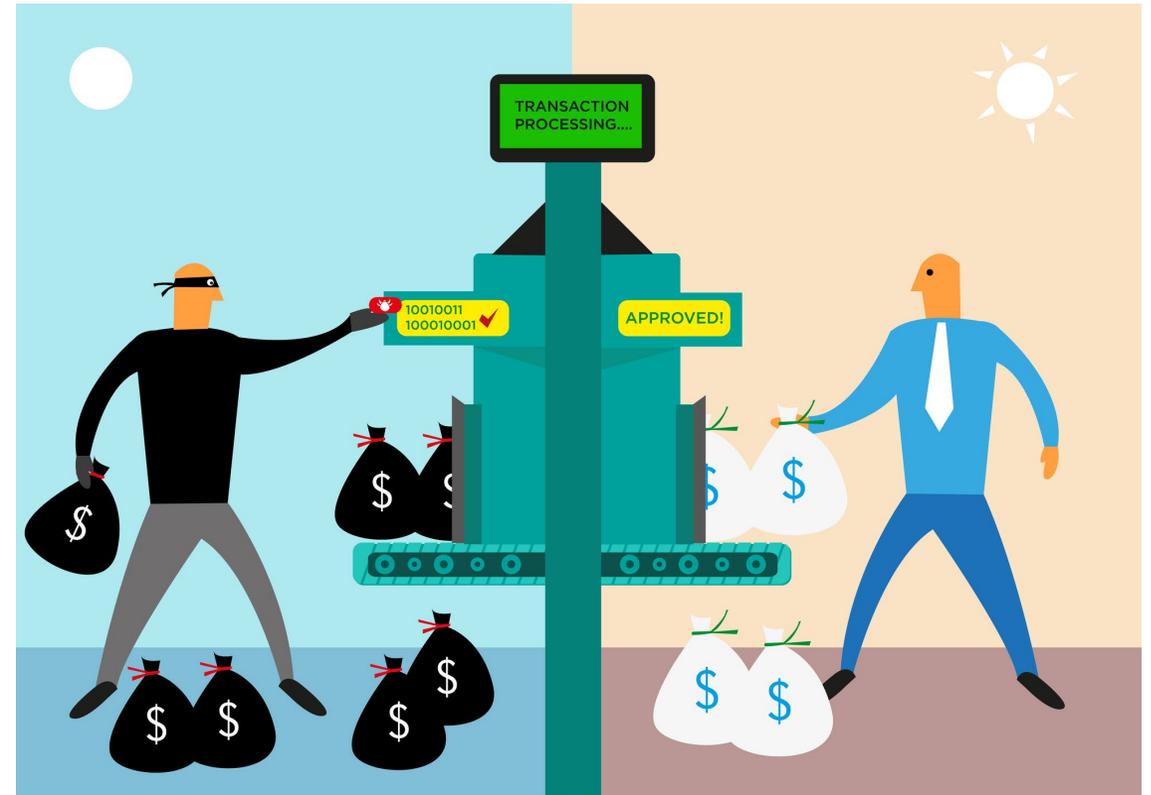
To put it simply, your files will be decrypted, your data restored and kept confidential, and your systems will remain secure.

Try Royal today and enter the new era of data security!

We are looking to hearing from you soon!

Fraudulent Instruction

- Recent claim where county ACH nearly 200K to bad actor posing as vendor
- Posed as AP at two different vendors requesting payment on legitimate invoices



Release of PII



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

How Can Public Entities Protect Against Cyber Risk?



Do you have policies related to cybersecurity?

Yes

No

Adopt a Cybersecurity Policy

MFA (Multi-Factor Authentication)



"Based on our studies, your account is more than 99.9% less likely to be compromised if you use MFA,"

[Alex Weinert](#)

Group Program Manager for Identity Security and Protection Microsoft.

EDR/XDR

- Anti-virus no longer enough
- Stop lateral movement
- Automated network isolation
- Behavior based, rather than definition based



Immutable Geo-Diverse Backups

Backups should be:

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

CIS



Training

CIS' learning center offers online cyber security awareness training

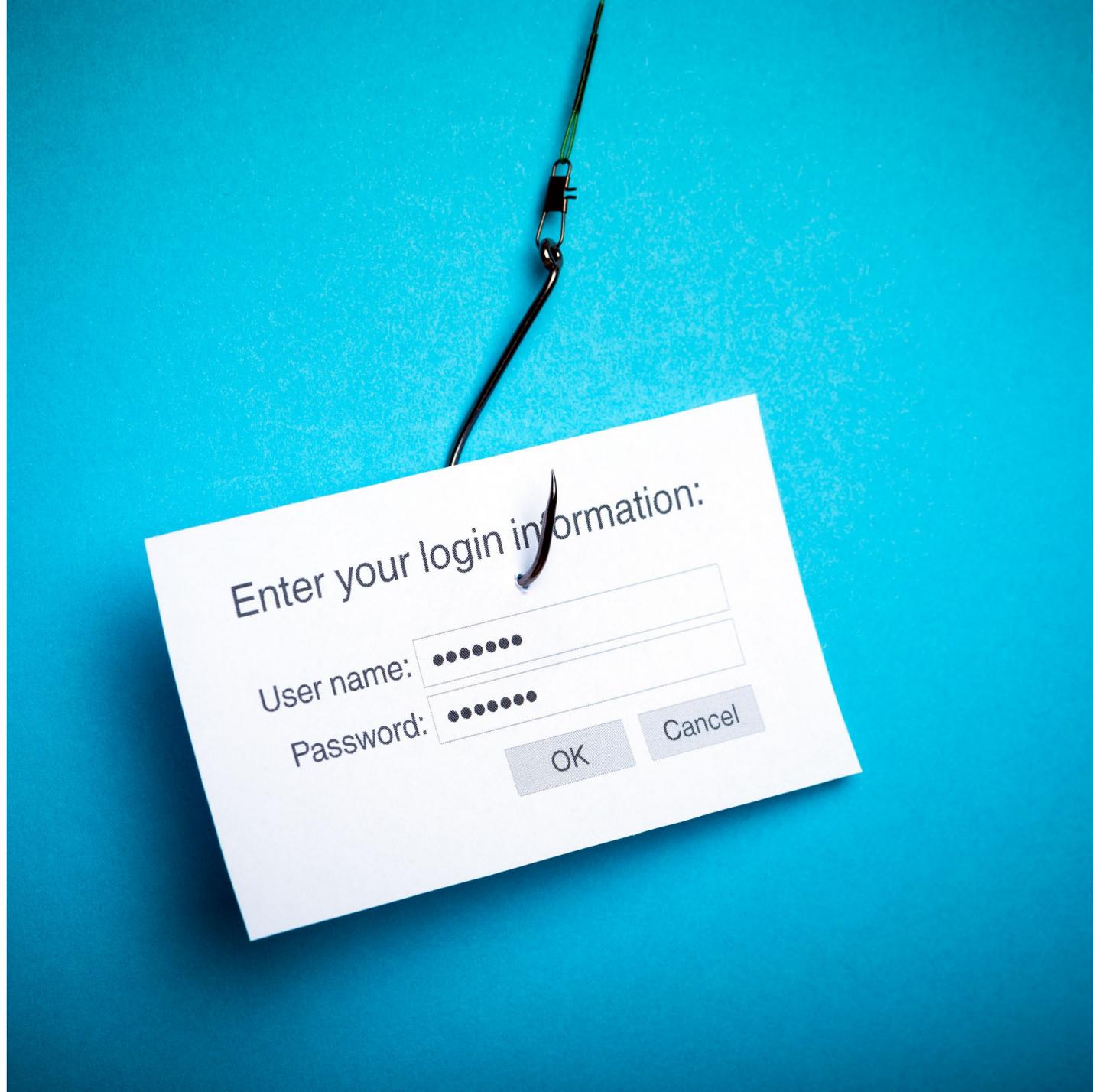


 <p>Cyber Security: Phishing Prevention Course (1 class) Phishing is one of the most dangerous and common cyber security risks today. This module takes a close look at the different types of phishing and provides tips to help you avoid being caught out. Objectives: Learn about the different types of phishing ...more</p> <p>★★★★★ LAUNCH ▼</p>	 <p>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</p> <p>★★★★★ PRINT CERTIFICATE ▼ View credits</p>	 <p>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</p> <p>★★★★★ LAUNCH ▼</p>
 <p>Cyber Security for the End User Course (1 class) By some estimates, over 90% of security breaches can</p> <p>★★★★★ LAUNCH ▼</p>	 <p>Cyber Security Essentials: Stop. Think. Ask.™ Course (1 class) Cybersecurity is the practice of protecting systems</p> <p>★★★★★ LAUNCH ▼</p>	 <p>Cyber Security: Risks and Social Media (Global) Course (1 class) This course discusses how social media affects you and</p> <p>★★★★★ LAUNCH ▼</p>

Phishing Exercises or Social Engineering Tests



88% of data breaches come from human error



Require Complex Passwords

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



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 white input field contains the password '123456'. To the right of the input field is a dark blue button with a white eye icon and the text 'pwned?'. Below the input field, a dark red banner contains the following text: 'Oh no — pwned!', 'This password has been seen 24,230,577 times before', and 'This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!'.

Vulnerability Scanning



Cyber Hygiene Scan

Web Application Scan

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



Purchase Cyber Insurance Coverage (from CIS)



CIS Cyber Coverage

3 Tiers

- Tier 1 – 50K
- Tier 2 – 250K
- Tier 3 – 1.25M

Participation

83% or 65% of population

- Tier 1 – 65%
- Tier 2 – 20%
- Tier 3 – 19%

Defining the Coverage Terms

- Business Interruption
- Cyber Extortion Loss (Ransomware)
- Data Recovery Costs
- Reputational Loss
- Data & Network Liability
- Regulatory Defense & Penalties
- Fraudulent Instruction
- Funds Transfer Fraud
- Telephone Fraud
- Breach Response

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
TIER 3	\$250,000	\$500,000	\$750,000	\$1,000,000
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	\$250,000	\$250,000	\$250,000	\$250,000
Funds Transfer Fraud	\$250,000	\$250,000	\$250,000	\$250,000
Telephone Fraud	\$250,000	\$250,000	\$250,000	\$250,000
Breach Response	\$500,000	\$750,000	\$1,000,000	\$1,250,000
Deductible	\$5,000	\$5,000	\$5,000	\$5,000



Cyber Coverage Requirements Tier 2 & Tier 3

- CIS Property Coverage
- Complete Application
- Cyber Security Policy
- One off-site backup
- Cyber Security Training
- CIS Excess Crime Coverage



How Can You Help?

- State and Local Cyber Grant funding for MFA and EDR
- Provide a state resource or fund for:
 - Breach coaching
 - Forensics
 - Data recovery

The state police have a forensics crime lab. **What about cyber forensics?**

Contact Info

Greg Hardin

Cybersecurity Specialist/
Systems Architect

503-763-3889

ghardin@cisoregon.org

