MANAGING HIDDEN CYBERSECURITY RISKS

Tony Giles & Rhia Dancel

NSF-International Strategic Registration

NSF-ISR
789 N. Dixboro Road, Ann Arbor, Michigan 48105 USA

Graphic elements sourced from 123RF.com

Agenda

- Top Identified Risks
- Best Practices in Risk Treatment
- Hidden Risks Organizations Face
- Q & A and Examples

About the Speakers

Tony Giles: Tony is an ISO 27001, ISO 20000 and ISO 9001 Lead Auditor and PenTester for NSF. Currently, Tony is the Director of Custom Audit Programs, also having served as Director of Operations, Director of Business Development and Service Delivery Manager. Tony has conducted audits globally for over 10 years and worked on large-scale security implementation projects, including NIST 800-171, NIST 800-88, ISO 27001, ISO 28000, PenTesting Assessments and other custom security standards. Tony has conducted audits for DoD Suppliers and Private Sector organizations implementing security assessment programs focused on multiple security controls, cryptographic erasure and other custom security programs. Tony has worked throughout the US advancing and building information security awareness.

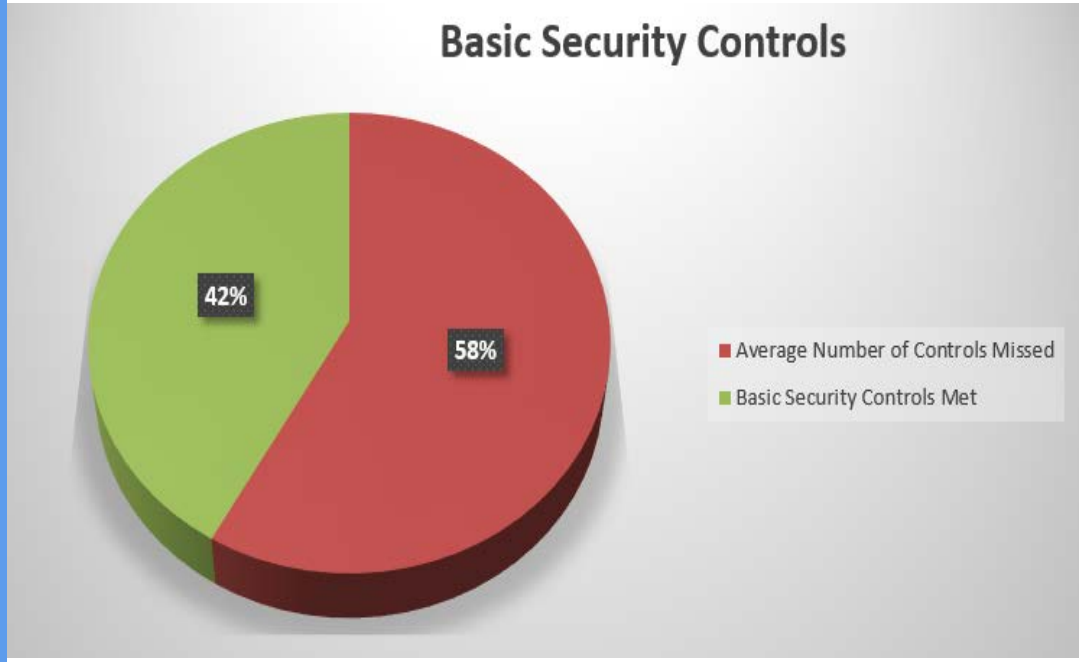
Rhia Dancel: Rhia is an ISO 27001 and 9001 Lead Auditor and PenTester for NSF and has previously held several auditing and technical positions in the information security and Pharma quality sectors. Rhia has completed technical writing work and audits for NSF throughout North America, working directly with customers on-site and remotely developing security control matrices. Rhia conducts risk-based security assessments using impact and probability calculations to develop and establish risk matrices to drive an organizations security plan-of-action and milestones. Rhia has developed and built a risk-based platform that supports industry best practices for treating and mitigating risk. Rhia has worked with multiple academic leaders on information security and awareness.

Basic Cybersecurity Risks

Top Known Cybersecurity Risks

1. Failure to Review Security Basics
   - Patching
2. Understanding What Creates a Risk
   - Phishing, DDoS Attack, Business Risk
3. Compliance is Not Security
   - Cybersecurity Policies
4. People/Team Members
   - First line of defense
5. Mobile Environment
   - Device Encryption
6. Funding
   - Where Do We Spend Money
7. Security Training
   - No Awareness Training
8. Lack of Recovery Plan
   - Data Lost or Not Accessible
9. Static Risk Assessments
   - Risk Is Dynamic
10. Infrastructure
    - Device Encryption

Top Known Cybersecurity Risks



- Research conducted on NIST 800-171 gap assessment revealed
  - Initial gap assessments revealed organizations on average missed 18 basic security controls
    - 31 basic security controls in place
  - Organizations only meet 42% of the basic security requirements

Top Known Cybersecurity Risks

- Most prevalent missed basic security controls/control families in NIST 800-171
  - Awareness and Training 2/3
  - Incident Response 2/3
  - Security Assessment 4/4
- The top three missed security control families all correlate back to the top-known cybersecurity risks

Risk Treatment Best Practices

Risk Treatment and Best-Practices

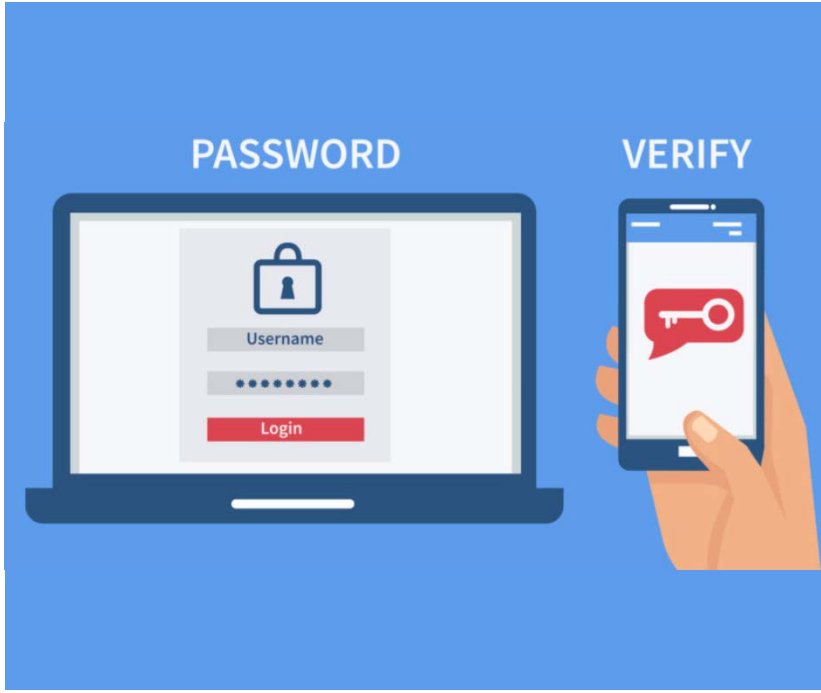
- Use the organization's risk assessment to prioritize risks mitigation
  - Focus on highest risks identified and progress accordingly
- Compare likelihood/probability/impact
- **How much does your risk treatment reduce your residual risk**
- Risk is unavoidable
- Use *Likelihood* and *Level of Impact* in NIST 800-30 as your Risk Assessment Scale

TABLE I-2: ASSESSMENT SCALE – LEVEL OF RISK (COMBINATION OF LIKELIHOOD AND IMPACT)

Likelihood (Threat Event Occurs and Results in Adverse Impact)	**Level of Impact**				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Risk Driving Continuous Improvement

- Remediate vulnerabilities in-line with the risk assessment
  - Higher vulnerabilities get higher prioritization
- Periodically assess risk
  - Risk changes – significant changes require updated risk assessment
  - Periodically assessing risk allows for organizations to continuously monitor their risk environment
- Scan the system environment
  - Logical and physical scan
- 1/3 of the basic security controls in NIST 800-171 is related to Risk



Risk Treatment and Best Practices

1. Security Patches
2. Organization Awareness
3. Outsourcing Managed Services
4. Risk Governance and Separation of Duties
5. Basic Security Controls
6. C-Suite Commitment
7. Employee Training
8. Data Storage Needs
9. Risk Assessment
10. Two-Factor Authentication
    - Google is protecting a staff of 85,000 employees with 2FA

The Hidden Risks

Hidden Risks Within Our Source Code

```
<iframe height='0' src='//www.googletagmanag
</noscript>
<script>
  window.ANALYTICS_DATA = {
    campaignData: '_band_1',
    seoContent: 'v10_FC_BR_FP',
    trackPageViewKey: '/analytics/name_resul
    pageController: 'v10/name',
    pageAction: 'search',
    stubGa: false,
    enableNewrelic: true,
    newrelicAppId: '25359015',
    validRoutes: true,
    enableSnowplowTracking: true,
    snowplowScript: 'https://assets.producti
    userId: '',
    trackingApiUrl: 'd21an0kpob.execute-api.
    uaKey: 'UA-45987076-1',
    gaKey: 'UA-9284963-2',
    gtmContainerId: 'GTM-5MHFDP',
    noResults: false,
    noResultsType: 'name',
    query: "John+Smith",
    isHiddenProfile: 'false',
    analytics: {"page_category":"name","page
  }
</script>
```

- We always start the process with foot-printing
  - This is intelligence on the identified organization
- Open Source Intelligence allows for hidden risks to be identified
- Hundreds of databases with API's and Demo's left open
- Wireless Networks to scan for a MAC address

Hidden Risks Within Our Social Media

A picture or video taken at just the right angle can reveal a lot…

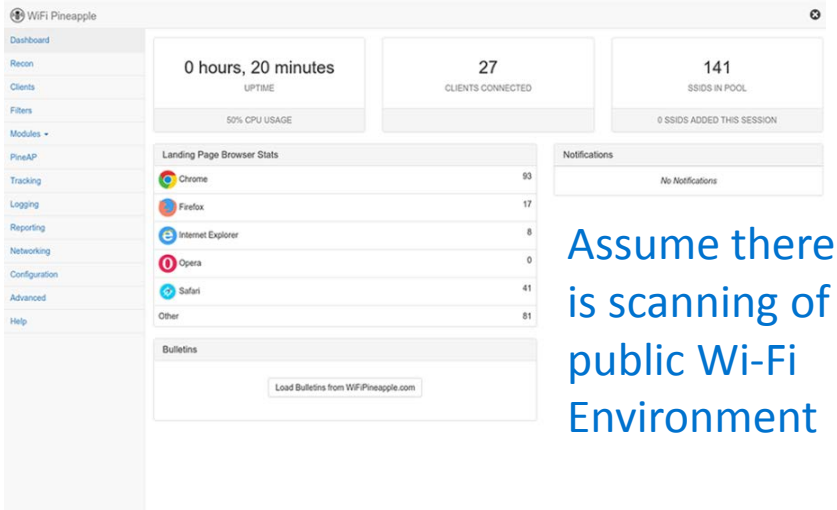
- Mobile device users - passwords
- ITAR drawings
- Usernames

Hidden Risks in the Live Environment

What are the risks associated with the below computer?

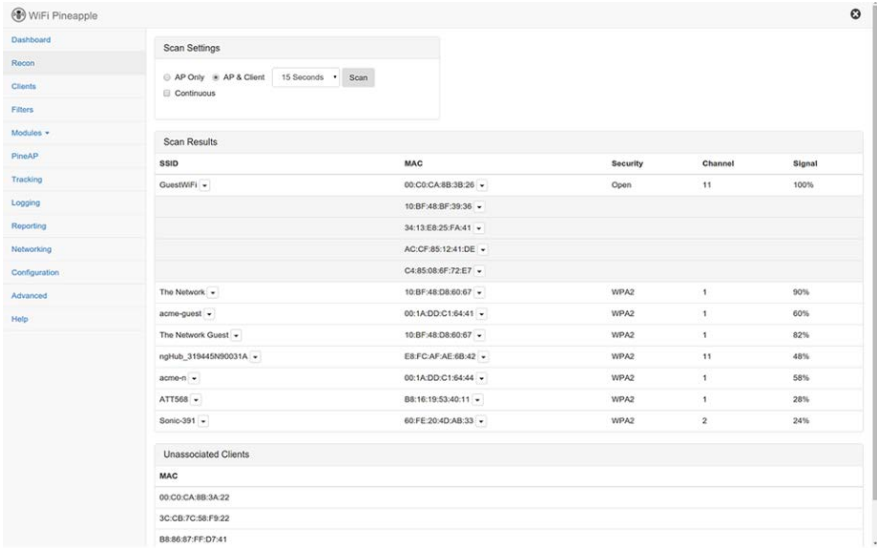
Let's have a demo of a public computer risk

Hidden Risks in the Live Environment



Assume there is scanning of a public Wi-Fi Environment

Recon work is done scanning the wireless environment



Thank You

Questions?

Tony Giles
Director of Custom Audit Programs, NSF-ISR
agiles@nsf.org

Rhia Dancel
Technical Scheme Manager, NSF-ISR
rdancel@nsf.org