October 2, 2018

Translating a lifetime of learning into cyber risk management

Bruce Potter
Don’t believe anything I say

• Fancy term – autodidact
• Real-life term – College dropout

• CISO of Expel, an MDR/MSSP based in Herndon, VA
• Founder – The Shmoo Group, help run ShmooCon
How do we make risk decisions?
Risk = Likelihood $\times$ Impact

Calculating Risk-Reduction ROI

Reduction in risk : $5 \times \$35,000 \times 0.85 = \$148,750$

ROI : $\frac{\$(148,750 - 25,000)}{25,000} = 4.95$

Savings per year : $\$25,000 \times 4.95 = \$123,750$

“You’re able to make risk decisions on the fly because of all the crazy experiences you’ve had.”
#1 Intelligent risk taking
“Kentucky windage” works pretty well for most cyber risk decisions

NOTE: That doesn’t mean your cyber risk management program should use “YOLO” as its core strategy

https://www.thoughtco.com/using-your-finger-like-a-weathervane-3444499
Total RAM = 1.25GB
<table>
<thead>
<tr>
<th>Slack</th>
<th>76.7 MB</th>
<th>29.9 MB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slack Helper</td>
<td>87.0 MB</td>
<td>41.3 MB</td>
</tr>
<tr>
<td>Slack Helper</td>
<td>156.5 MB</td>
<td>87.1 MB</td>
</tr>
<tr>
<td>Slack Helper</td>
<td>678.7 MB</td>
<td>420.8 MB</td>
</tr>
<tr>
<td>Slack Helper</td>
<td>327.5 MB</td>
<td>146.6 MB</td>
</tr>
</tbody>
</table>

Total RAM = \( \sim 1.25 \text{GB} \)
You can do a lot with a little.
Modern systems have immense capability. “Live off the land” when it comes to risk management.

- Vuln scanner = asset management
- Web logs = mobile device policy auditing
- ELK stack = all things to all people ;)

“A penny saved is a penny earned.”
But sometimes…

- The opportunity cost of living off the land is too high or
- The capability is not mature enough.

**Buy the right tool in those cases.**
The Internet has revolutionized commerce and payment processing.
#3 Tie security to business drivers*  
*appropriately
The amount of security you have needs to be appropriate to the business you are in:

- Probably doesn’t need to be world class
- Probably needs to be better than your peers

Be wary of dramatically over achieving in your risk program
The Shmoo Group
Never get complacent
This industry constantly changes

Acceptable risk today may not be acceptable tomorrow

Hold people accountable, including yourself

A good risk program is one that always challenges itself
WELCOME TO VIRGINIA

VIRGINIA IS FOR LOVERS
#5 Be humble
It leads to better risk decisions

- You will listen more
- You will learn more
It leads to better risk programs

- Security will not be viewed as an end in and of itself
- Your team will have better relationships with the rest of the business
Booz | Allen | Hamilton
See life from different verticals
Diversity in experience = A better risk program

- Encourage people to get out of the office
- Visit other parts of the company
- Go to conferences, talk to peers
Pont Tec

Pont Tec Technologies is a services-based company focused on developing operational IT security solutions, crafting IT security strategies, and deploying advanced defensive capabilities. We focus on research and leading edge technologies, and we assist organizations in bringing advanced defensive technologies to bear on current IT security problems.

What We Do

We focus on research and leading edge technologies, secure software development, and assisting organizations in bringing advanced defensive technologies to bear on today’s hard IT security problems.

We provide talented, agile, research-focused staff with leading edge Information Assurance technology research experience. We develop software for both research tasks and production systems, and advise our clients on secure software development practices. We help people to understand what is going on in their networks, how their systems may have been compromised and how to regain control when all seems lost, and provide training on real-world cybersecurity challenges.

Our Value Proposition

As a private firm, Pont Tec is fast and flexible, able to quickly respond to the dynamic needs of its clients, partners, and market. Our agile nature enables Pont Tec to meet our clients’ most urgent needs, as well as to remain on the forefront of information security research.

Pont Tec provides competitive rates and impeccable service to our clients through our dedication to long-range staff development.

Contact us today to join our team or to find out how we can help you to achieve your mission:
info@ponte.com

Unique Expertise & Insight

With our headquarters in Ellicott City, MD, Pont Tec houses a unique combination of technical expertise, national security insight, and strong relationships with leading stakeholders in the Information Security and Intelligence Communities.
What does it take to run a small business?

- Payroll
- Recruiting
- Taxes
- Sales
- Facilities
- AP/AR
- Staff development
- Legal
- Compliance
- …
What does it take to run a risk program?

- Inventory and asset management
- Identity and asset management
- Network & endpoint controls
- Incident response
- DR/BC program
- Compliance
- Data at rest protection
- Data in transit protection
- …
#7 Be organized
...at an appropriate level for your org
Risk needs to be relatable
... to your exec team
... to your board
... to your staff
... to all employees
Risk needs to be aligned
CISOs should report to the highest point of accountability possible
Tired …

CISO and Security are subordinate to CIO and IT

Wired …

CIO and IT are subordinate to CISO
When you start like this from the beginning, security is an integrated part of your culture.
NIST CSF Self-scoring tool and “getting started” guide

expel.io/nist
Run your IR table-top exercises D&D-style

expel.io/ohnoes