a presentation by saumil shah
hitbgsec2019 singapore
special thanks to

DR. IGOR PODEBRAD
KELLY WHITE
ANOOP SEHTI
HIREN SHAH
THOMAS DULLIEN
A TALE OF TWO KEYNOTES
ATTACKS ARE A TECHNICAL PROBLEM, DEFENSE IS A POLITICAL PROBLEM

THOMAS DULLIEN, "Why we are not building a defendable Internet" BH ASIA 2017
DEAR CISO,
WHO ARE YOU MOST SCARED OF?

SAUMIL SHAH
"The Seven Axioms Of Security"
BH ASIA 2017
DILEMMA:

ATTACKERS or AUDITORS?
The Seven Axioms of Security

1. CISO - Defend the organization.
2. Threat Intel - Collect Everything.
3. Test Realistically.
5. Users - One Size Fits NONE!
Cybersecurity Pros Name Their Price as Hacker Attacks Swell.

One example— a $650k salary for a CISO role last year, required $2.5m to fill this year. There are 300,000 unfilled cybersecurity jobs in the U.S. last year alone. 

#Infosec #CISO
zc.io/kf84 @business

Cybersecurity Pros Name Their Price as Hacker Attacks Swell

By Anders Melin
August 7, 2019, 7:00 AM EDT
Updated on August 7, 2019, 8:46 AM EDT

- ‘A full-on war for cyber talent,’ executive recruiter says
- Average digital breach costs firms $8 million, study finds

It took a $650,000 salary for Matt Comyns to entice a seasoned cybersecurity expert to join one of America's largest companies as chief information security officer in 2012. At the time, it was among the most lucrative offers out there.

This year, the company had to pay $2.5 million to fill the same role.
LIFE'S A BEACH!
Any HIGH and MEDIUM severity vulnerabilities should be investigated and confirmed so that remediation can take place. LOW risk items should not be ignored as they can be chained with other vulnerabilities to enable further attacks.

Vulnerability Summary

<table>
<thead>
<tr>
<th>Severity</th>
<th>Description</th>
<th>CVSS Count</th>
<th>Likelihood</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Webmin &lt;= 1.900 RCE Vulnerability</td>
<td>9.0</td>
<td>E</td>
<td>6</td>
</tr>
<tr>
<td>High</td>
<td>HTTP Brute Force Logins With Default Credentials Reporting</td>
<td>9.0</td>
<td>D</td>
<td>5</td>
</tr>
<tr>
<td>Median</td>
<td>Webmin 1.880 Information Disclosure Vulnerability</td>
<td>5.0</td>
<td>C</td>
<td>4</td>
</tr>
<tr>
<td>Median</td>
<td>Cleartext Transmission of Sensitive Information via HTTP</td>
<td>4.8</td>
<td>B</td>
<td>3</td>
</tr>
<tr>
<td>Median</td>
<td>SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabilit...</td>
<td>4.0</td>
<td>A</td>
<td>2</td>
</tr>
</tbody>
</table>
LIFE'S A BEACH!
DILEMMA: ^C

x 2  WORLD 2-1
Understand the relationships

REGULATORS

CISO

IT VENDORS

BOARD

YOUR TEAM
Security products

Why is there a market for this?

- CISO needs to make purchasing decisions in a market full of poor products.
- Biggest risk to CISO is being seen as “having forgotten” a risk
- Solution is often portfolio purchase: “Buy one of each product category”
Dino A. Dai Zovi @dinodai... · 5m

The problem with toil is that it's addictive. You feel like you are making progress because you are busy fighting fires.

If your security team is created from people who prefer toil to writing code, you'll never be able to scale with software.
SHOULDERS OF GIANTS

ANOOP SETHI
formerly BT

KELLY WHITE
formerly Zionsbank

Dr IGOR PODEBRAD
Commerzbank AG
THERE IS A WAY
HAVE NOTS

Not capable
Cyber Security is a necessary evil
Purely dependent upon commercial solutions

HAVES

Capable of custom analytics threat detection and response
Owning Cyber Security
Sucked up all the talent

CYBERSECURITY ASYMMETRY DILEMMA
BUILD SWARM INTELLIGENCE
Spiral Dynamics
Spiral Dynamics

HIVE MIND
The swarm will learn and overcome any obstacle
The Leader is the CATALYST
SELECT THE GOALS WORTH FIGHTING FOR
The Downward Spiral

Cascade Effect

Doesn't take much to de-orbit

It all hinges upon the LEADER
Nurturing the Spiral

The Leader's Reflection

PROTECT the Swarm

EMPOWER the Swarm

Form strong PARTNERSHIPS
Catalyst
- Listen more than you speak
- Build capabilities
- Strong relationships with the business

Authoritative
- Behave in a superior way over their team-mates
- Fight the business
- The "Sky Is Falling"
A CENTRE OF EXCELLENCE FOR ALL OF TECHNICAL SECURITY

An Independent Consultancy within the organisation
PROTECT THE SWARM

Creative Insulation

HONESTY and OPENNESS

⚠️ Happens

Don't throw them under the bus!

No Blank Cheques
Once you hire two toxic people, they hire all their other toxic friends and destroy everything.

09:22 · 21/08/19 · Twitter Web App

home skillet @ralph_squilla... · 1d
Replying to @rakyll
Blockchain of toxic
EMPOWER The Swarm

Call you out on your bull💩
PARTNERSHIPS

SURROUND YOURSELF WITH SMART PEOPLE IN SMALL TEAMS
THE TALENT WILL COME TO YOU
THE CISO'S DILEMMA

YOU ALWAYS HAVE A CHOICE.

YOUR OWN SIDE   THE TEAM'S SIDE
THE CISO'S DILEMMA

YOU ARE ALWAY HAVE A CHOICE.

YOUR OWN SIDE

THE TEAM'S SIDE
ALL ALONE AND NO WAY OUT
thank you
@therealsaumil