INTRODUCTION AND A LOOK AT SECURITY TRENDS

Hugh Thompson, Ph.D.
Program Committee Chairman, RSA Conference
WELCOME TO THE PADANGTEGAL
MANDALA WISATA WANARA WANARA
SACRED MONKEY FOREST SANCTUARY

DEAR VISITORS,
ON BEHALF OF THE VILLAGE OF PADANGTEGAL AND THE WANARA WANARA FOUNDATION, WE WISH YOU AN ENJOYABLE AND EDUCATIONAL VISIT TO OUR FOREST, MONKEY FOREST, AND TEMPLE COMPLEX. TO ENJOY A MEMORABLE VISIT PLEASE OBSERVE THE FOLLOWING:

1. THIS IS A SACRED AREA. PLEASE COMPORT YOURSELF WITH RESPECT FOR THE PEOPLE WHO WORSHIP HERE, THE TEMPLES, AND THE MONKEYS AND OTHER PLANTS AND ANIMALS THAT RESIDE IN THE FOREST.

2. THE MONKEYS OF THE FOREST (MACAQUE AND TIBETAN MACAQUE) ARE WILD ANIMALS. PLEASE REFRAIN FROM TOUCHING OR PLAYING WITH THEM, AS IT MIGHT CAUSE THEM AN UNPLEASANT SURPRISE. MONKEYS DO NOT PROVIDE TREATS FOR THE MONKEYS AS THEY ARE A PROTECTING MOTHER, EVER KEEP A SAFE DISTANCE FROM MONKEYS AT ALL TIMES.

3. PLEASE READ THE BROCHURE PROVIDE WITH THE ENTRANCE TICKET FOR FURTHER INFORMATION ABOUT THE SANCTUARY.

WE THANK YOU FOR FOLLOWING THESE REGULATIONS AND WE TRUST THAT YOUR VISIT WILL BE A MEMORABLE ONE.

Sincerely,

WANARA WANARA FOUNDATION
RISK
Agenda

Intro to Information Security

Economics of Information Security

Security Trends
The Shifting IT Environment

(...or why security has become so important)
The business has to adhere to regulations, guidelines, standards,…
- SAS 112 and SOX (U.S.) – upped the ante on financial audits (and supporting IT systems)
- PCI DSS – requirements on companies that process payment cards
- HIPAA, GLBA, GDPR, …, many more

Audits have changed the economics of risk and create an “impending event”

Hackers *may* attack you but auditors *will* show up

Disclosure laws mean that the consequences of failure have increased
- Waves of disclosure legislation
Shift: Technology

- Many applications/transactions now operate over the web
- Cloud has changed our notion of a perimeter
- Worker mobility is redefining the IT landscape
- Shadow IT is becoming enterprise IT
- Majority of web transactions are now encrypted (SSL)
- The security model has changed from good people vs. bad people to enabling partial trust
  - There are more “levels” of access: Extranets, partner access, customer access, identity management, …
Shift: Attackers

- Many cyber criminals are organized and profit-driven
  - An entire underground economy exists to support cybercrime
- Attackers are shifting their methods to exploit both technical and human weaknesses
- Attackers after much more than traditional monetizable data (PII, etc.)
  - State-sponsored attacks
  - Influence
  - Hacktivism
  - IP attacks/breaches
Customers, especially businesses, are using security as a key discriminator.

Security has become a non-negotiable expectation of businesses.

Security is being woven into service level agreements (SLAs).

The “average person” is now familiar with security.
Big Questions

- How do you communicate the value of security to the enterprise (and management)?
- How do you measure security?
- How do you rank risks?
- How do you reconcile security and compliance?
- How do you adapt to paradigms like IoT?
- How can you be proactive and not reactive? What is “threat intelligence” and how would you actually consume, act on or share it?
- What changes are likely in privacy laws, data sovereignty, trust?
- What about big issues in the news like breaches of very personal data that cannot be reset or revoked? How should/can we adapt what we do based on them?
The Economics of Security
Hackernomics (*noun*)

A social science concerned chiefly with description and analysis of attacker motivations, economics, and business risk. Characterized by **5 fundamental immutable laws and 4 corollaries**
Law 1

Most attackers aren’t evil or insane; they just want something

Corollary 1.a.:
We don’t have the budget to protect against evil people but we can protect against people that will look for weaker targets
Law 2

Security isn’t about security. It’s about mitigating risk at some cost.

Corollary 2.a.:
In the absence of metrics, we tend to over focus on risks that are either familiar or recent.
Law 3

Most costly breaches come from simple failures, not from attacker ingenuity

Corollary 3.a.:
Bad guys can, however, be VERY creative if properly incentivized.
The CAPTCHA Dilemma

Completely Automated Public Turing test to tell Computers and Humans Apart
Law 4

In the absence of security education or experience, people (employees, users, customers, ...) naturally make poor security decisions with technology.

Corollary 4.a.:

Systems need to be easy to use securely and difficult to use insecurely.
Law 5

Attackers usually don’t get in by cracking some impenetrable security control, they look for weak points like trusting employees
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>web 2.0</td>
<td>web 2.0</td>
<td>data</td>
<td>real–world</td>
<td>BYOD</td>
<td>APT</td>
<td>BYOD</td>
<td>IoT</td>
<td>IoT</td>
<td>ransomware</td>
<td>ransomware</td>
</tr>
<tr>
<td>network access control</td>
<td>anti–virus</td>
<td>risk</td>
<td>real–time</td>
<td>tablet</td>
<td>BYOD</td>
<td>IoT</td>
<td>threat actors</td>
<td>ransomware</td>
<td>ransomware</td>
<td></td>
</tr>
<tr>
<td>anti–virus</td>
<td>social networking</td>
<td>organizations</td>
<td>cloud–based</td>
<td>APT</td>
<td>security analytics</td>
<td>security analytics</td>
<td>BYOD</td>
<td>devops</td>
<td>GDPR</td>
<td></td>
</tr>
<tr>
<td>cross–site scripting</td>
<td>access</td>
<td>third–party</td>
<td>anti–virus</td>
<td>mobile apps</td>
<td>threat actors</td>
<td>security analytics</td>
<td>threat actors</td>
<td>iot devices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCI–DSS</td>
<td>PCI–DSS</td>
<td>compliance</td>
<td>in–depth</td>
<td>MDM</td>
<td>software–defined</td>
<td>home depot</td>
<td>kill chain</td>
<td>kill chain</td>
<td>devops</td>
<td></td>
</tr>
<tr>
<td>sarbanes oxley</td>
<td>myspace</td>
<td>key</td>
<td>high–profile</td>
<td>iOS</td>
<td>MDM</td>
<td>snowden</td>
<td>devops</td>
<td>GDPR</td>
<td>blockchain</td>
<td></td>
</tr>
<tr>
<td>service–oriented</td>
<td>conficker</td>
<td>attacks</td>
<td>real–life</td>
<td>stuxnet</td>
<td>iOS</td>
<td>software–defined</td>
<td>OPM</td>
<td>blockchain</td>
<td>equifax</td>
<td></td>
</tr>
<tr>
<td>unified communications</td>
<td>VOIP</td>
<td>applications</td>
<td>Epsilon</td>
<td>Flame</td>
<td>stuxnet</td>
<td>data science</td>
<td>software–defined</td>
<td>cyber insurance</td>
<td>wannacry</td>
<td></td>
</tr>
<tr>
<td>javascript</td>
<td>payment card</td>
<td>control</td>
<td>end–user</td>
<td>mobile apps</td>
<td>tablets</td>
<td>devops</td>
<td>NIST CSF</td>
<td>security analytics</td>
<td>threat hunting</td>
<td></td>
</tr>
<tr>
<td>management strategy</td>
<td>ratio</td>
<td>process</td>
<td>enterprise–wide</td>
<td>advanced malware</td>
<td>prism</td>
<td>heartbleed</td>
<td>iot security</td>
<td>NIST CSF</td>
<td>bitcoin</td>
<td></td>
</tr>
<tr>
<td>PDAs</td>
<td>PDAs</td>
<td>security standard</td>
<td>enterprise</td>
<td>zero–day</td>
<td>kill chain</td>
<td>advanced malware</td>
<td>kill chain</td>
<td>anthem</td>
<td>dark web</td>
<td></td>
</tr>
<tr>
<td>email security</td>
<td>data security</td>
<td>environment</td>
<td>cost–effective</td>
<td>software–defined</td>
<td>dropbox</td>
<td>ransomware</td>
<td>dark web</td>
<td>bitcoin</td>
<td>devsecops</td>
<td></td>
</tr>
</tbody>
</table>

Source: Cyentia Institute with data from RSA Conference
Some hot areas...

- GDPR and data privacy
- Data sovereignty and legislative volatility
- The human element of security
- The potential application of blockchain technologies to security
- The application, potential and limitations of AI in security
Enjoy the rest of the conference!!
THANKS!

Hugh Thompson, Ph.D.
hugh_thompson@symantec.com