

AT&T Security Services

Risk reduction through vulnerability management

DuWayne E. Aikins Sr., PMP
Senior Strategist, CyberSecurity

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.



CIO/CISO questions and best practices

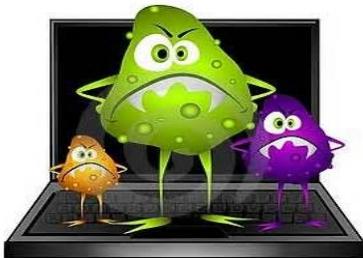
5 Questions every CIO/CISO should answer

- When did you and your staff review your last risk assessment?
- Why are you a target for attacks?
- What data is leaving your organization and is it secure?
- Is your employees fully engaged in cybersecurity?
- Does my security organization have all the tools and resources they need to help prevent a security breach?

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.



Threat Landscape



- Nine new pieces of malware are discovered Every Second
 - TRANSLATION: 12,960/Day
- 97% of fortune 500 companies have admitted they've been hacked
 - 60% of malicious hacks are for financial gain

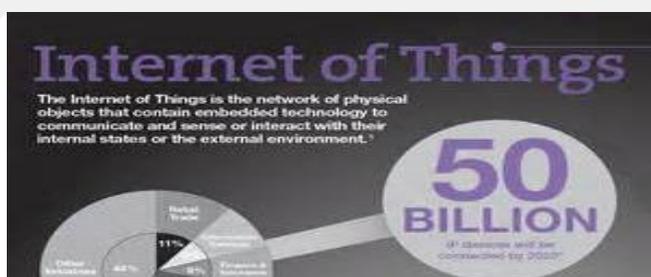


© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.

3



Threat Landscape



- Using internet enabled devices to operate our world.
- Shift from using the internet to communicate
- With 50 billion new devices connecting to the internet in the next 5 years, devices will be communicating with themselves
- Allows hackers to penetrate further into our lives

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.

4



Threat Landscape

Cyberspace, a Military Zone?

- 100 governments have created military units to fight and win cyber wars
- Terrorists Organizations are now involved in cyber attacks
- STUXNET
 - Computer worm designed to attack programmable logic controllers
 - Reportedly ruined almost one-fifth of Iran's nuclear centrifuges
- WIPER: Two destructive threads
 - Overwrites data
 - Interrupts execution processes

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.

5



People's Liberation Army, Unit 61398

- Since 2006, Mandiant has observed Unit 61398 compromise 141 companies spanning 20 major industries.
- Unit 61398 maintained access to victim networks for an average of 356 days. The longest time period Unit 61398 maintained access to a victim's network was 1,764 days, or four years and ten months.
- Of the 141 APT1 victims, 87% of them are headquartered in countries where English is the native language.
- The industries APT1 targets match industries that China has identified as strategic to their growth, including four of the seven strategic emerging industries that China identified in its 12th Five Year Plan.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.

6



We need to take a risk management approach



7

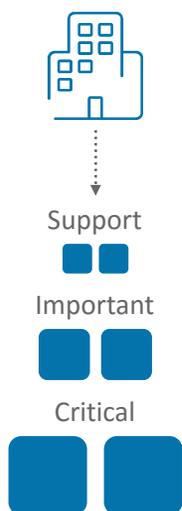
© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.



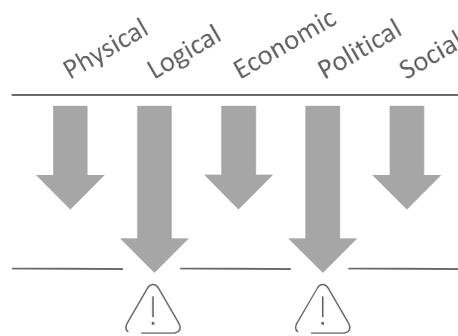
Start with assessment & governance

The risk management approach

Processes/assets
business values



Threats



Vulnerabilities



Risk

Probability that a threat will exploit a vulnerability

Exposure

Potential loss



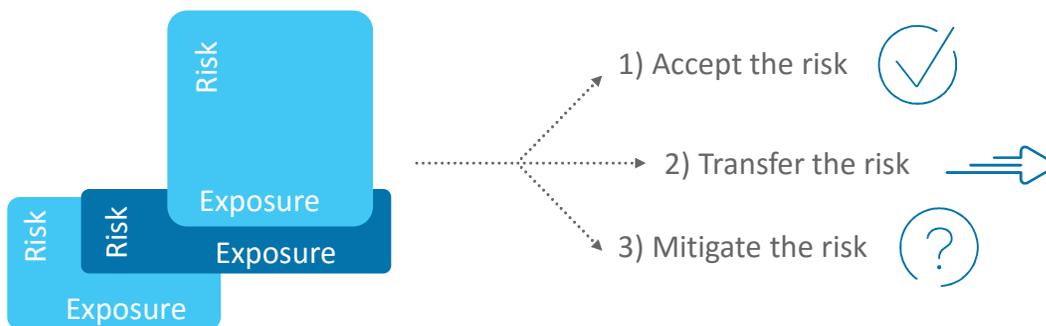
8

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.



The continuity challenge

Risk portfolio management options



The challenge

Maximize the value of the business by balancing costs and risks of disasters with the costs of preparedness and recovery/restoration.

Mitigation Impact



Mitigation Costs

- Threat reduction
- Vulnerability reduction
- Exposure reduction

9

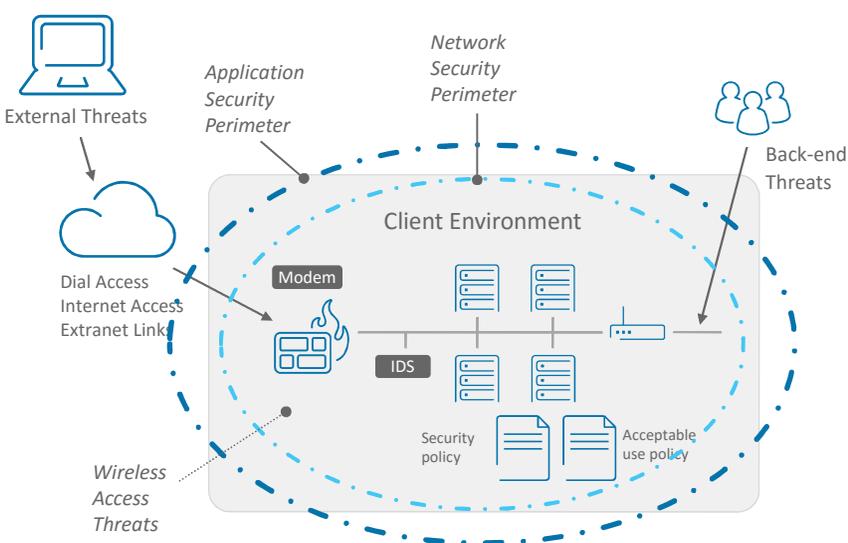
© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.



Security threats can originate from many places

Assets include:

- Business applications, web applications, e-business applications
- Internal systems / information repositories (hosts, servers, disk arrays, etc.)
- Internet connections, DMZs, internal networks
- Extranet connections to vendors & business partners



Security threats come from inside and outside the network edge

10

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.



Client-specific vulnerabilities & challenges

- Tele-workers using “always on” DSL and Cable connections
 - Current solutions typically engage Security procedures only when VPN client is engaged
 - Must enforce OS patches & AV signatures prior to access
- Employees using company assets for unapproved purposes
- Wireless LAN and their clients
 - Can broadcast your company data into adjacent buildings, public spaces, even competitors offices
- Patches
 - Difficult to test and deploy rapidly
- Anti-virus software
 - Reacts too late to block emerging threats
- Perimeter firewalls
 - Can’t inspect trusted VPN Traffic
- Intrusion detection systems
 - Detects but doesn’t block attacks

“Each (worm) variant released so far has exceeded the previous one in growth and impact during the critical initial window of vulnerability.”

SoBig.F Virus Breaks Speed Records, eWeek



Security threat, vulnerability, patch & asset process



Requirements

- Predictive information
- Knowledge
- Velocity of knowledge
- Knowledge of exploits
- Correlation of exploits
- Real-time data mining
- Capabilities
 - Correlation software
 - Daytona

Exploits



Known Un-known



Security

- Fixing software
- Policy adm.
- Password/auth. Mgmt
- Information protection
- Encryption/key mgmt

Operating systems

- Windows based
- Unix based
- Palm
- Blackberry
- Etc.



Platforms

- Mobility devices
- Pc's
- Pda's
- Various server
- Large



Vulnerability and threat management

Provides an independent baseline and validation of the organization's security posture. Can simulate real-world attacks to identify vulnerabilities in the network, evaluate risks, and develop remediation plans that are tailored to unique business requirements and security needs.

- Vulnerability management
- VoIP penetration testing
- Wi-fi penetration testing
- War dial
- Social engineering
- Mobile security assessments
- Denial of service based testing
- Virtualization security
- Remote access assessment
- Breach/incident response testing

Vulnerability assessments

- Scanning of the target infrastructure, establishing a baseline and making compliance easier by validating external posture
- Providing an overall security picture at a lower cost with repeatable exercises
- Periodically verifying assets are properly protected; evaluating recurring differentials and managing vulnerabilities

Penetration testing (aka ethical hacking)

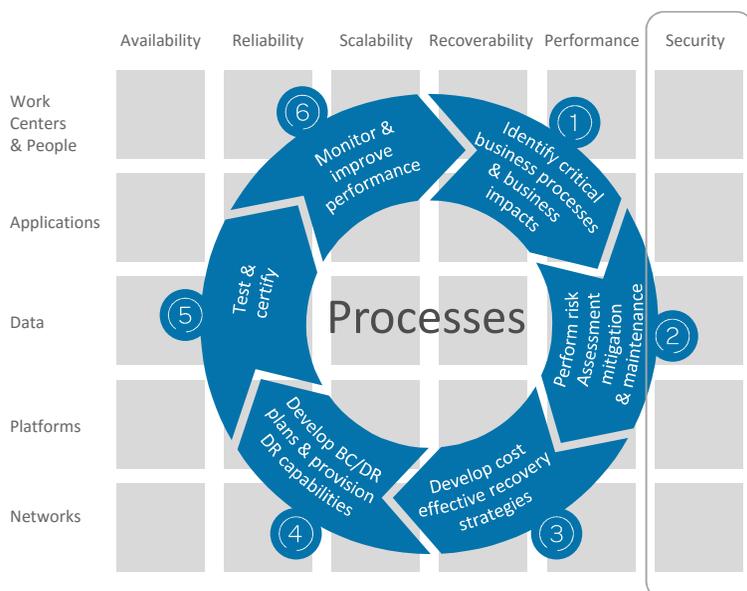
- Takes Vulnerability Assessment to the next level
- Manual testing and exploits, in addition to false positive reduction of automated results
- Taken from the perspective of a malicious external entity, or rogue internal resource
- Verifying that defense in depth and response capabilities are working as designed, along with security controls validation
- Required by many industry regulations and standards

13

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.



AT&T Best Practices: Proven methodology



- Incorporates industry leading elements of a cyber security architecture
- Addresses all three states of information: In motion, processing and at rest
- Addresses corporate, legislative & tactical policies necessary to govern
- Addresses traditional reactive elements of security architecture
- Incorporates new predictive elements of a security architecture

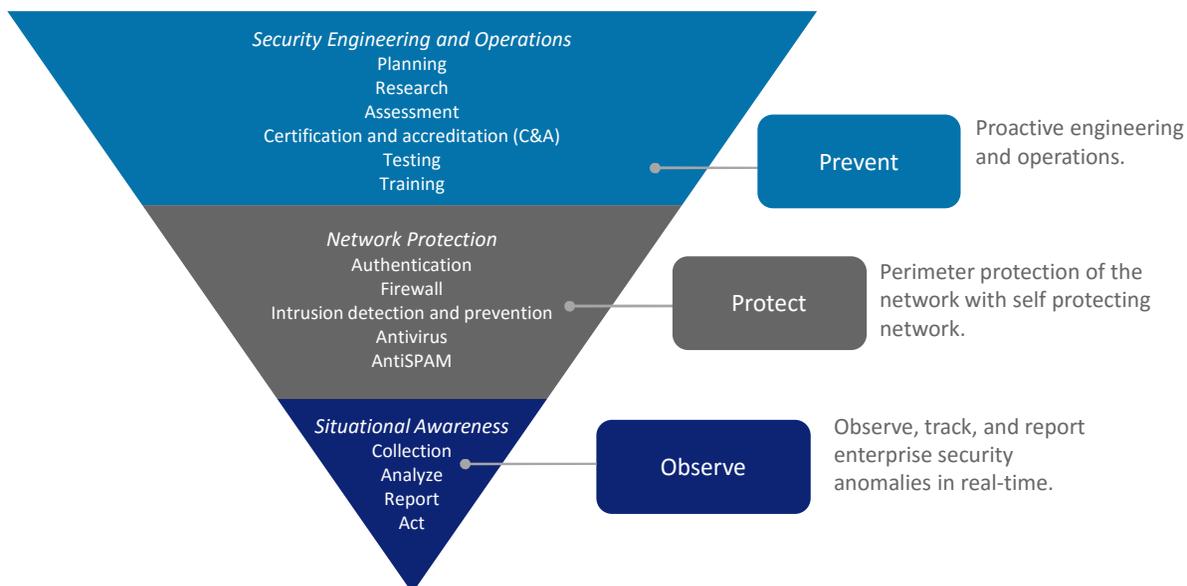
14

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.



AT&T approach for cyber security

Observe, protect, and prevent



15

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.



Security best practices

Risk-based approach

- Security must implemented based on threat and vulnerability assessments

Risk impacts

- Brand
- Revenue/regulation
- Intellectual property

Defense in depth

- Use multiple layers of defense

Security by design

- Security must be designed in the beginning; must be anticipatory and predictive

ROI/ROR

- Security must be efficient and cost effective; risk-mitigation has a positive bottom-line impact



16

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.



Conclusion

Highlighted best practices

- Make sure it is understood that security is everyone's job, including the executives
- Adopt a risk-driven approach to cybersecurity strategy
- Assess your data and assets from outside looking in to identify adversaries
- Appoint someone to champion data security
- Form an information security committee
- Evolve with technology: invest in capabilities and respond to evolving adversaries
- Get outside help: outside advisors help discover undetected vulnerabilities
- Lead by example: everyone is part of strong, effective cybersecurity policies

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.

17



18

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.