RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: TV-W12

GAME OF PWNS: THE PILLARS OF CYBER-RISK RESILIENCE

David Rusting

Chief Information Security Officer
University of California


CHAOS IS A LADDER.
MANY WHO TRY TO CLIMB IT FAIL,
AND NEVER GET TO TRY AGAIN.
THE FALL BREAKS THEM.
AND SOME ARE GIVEN A CHANCE TO CLIMB BUT THEY REFUSE.
THEY CLING TO THE REALM OR THE GODS OR LOVE
ILLUSIONS
ONLY THE LADDER IS REAL.
THE CLIMB IS ALL THERE IS.

THE UNIVERSITY OF CALIFORNIA AT A GLANCE

INFLUENTIAL SCALE[1]	
Campuses	10
Medical Centers	5
National Laboratories[2]	3
FTE Students	252,000
Full-time Faculty and Staff[3]	146,000
Living Alumni	1,700,000

5 ACADEMIC MEDICAL CENTERS[4]	
Licensed Beds	3,666
Outpatient Clinic Visits Annually	4,500,000
Inpatient Days Annually	972,000
Major trauma centers	5

HONORS & AWARDS	
Nobel Prizes – *most of any public university*	61
National Medals of Science	67
MacArthur Fellows	85
Fulbright Award Recipients	264
Pulitzer Prize Winners	16

STRONG GOVERNANCE AND INDEPENDENCE FROM THE STATE

President Janet Napolitano directly oversees the 10 campus chancellors and the director of the Lawrence Berkeley National Lab

UC remains constitutionally autonomous and is governed by a 26-member Board of Regents

1. Source: Annual Financial Report 2014-15; 2. UC operates and manages Lawrence Berkeley National Laboratory under a contract directly with the Department of Energy (DOE). The University is a member in two separate joint ventures that operate and manage two other DOE laboratories, Los Alamos National Laboratory and Lawrence Livermore National Laboratory.
3. As of October 31,2015; 4. Source: Medical Center Financial Report 2014-15.


WINTER IS COMING
STARK

The Question

"How do we protect our institution when the very nature of our mission is to be open?"

The Balance

Common challenges across UC

- ***Open environment***
- ***Distributed structure***
- ***Sensitive, valuable data***

Higher Risk	Lower Risk
Lower Cost	Higher Cost
Lower Maturity	Higher Maturity

"How have you created an appropriate level of security that balances our need to protect with our need to run the university and support its mission?"

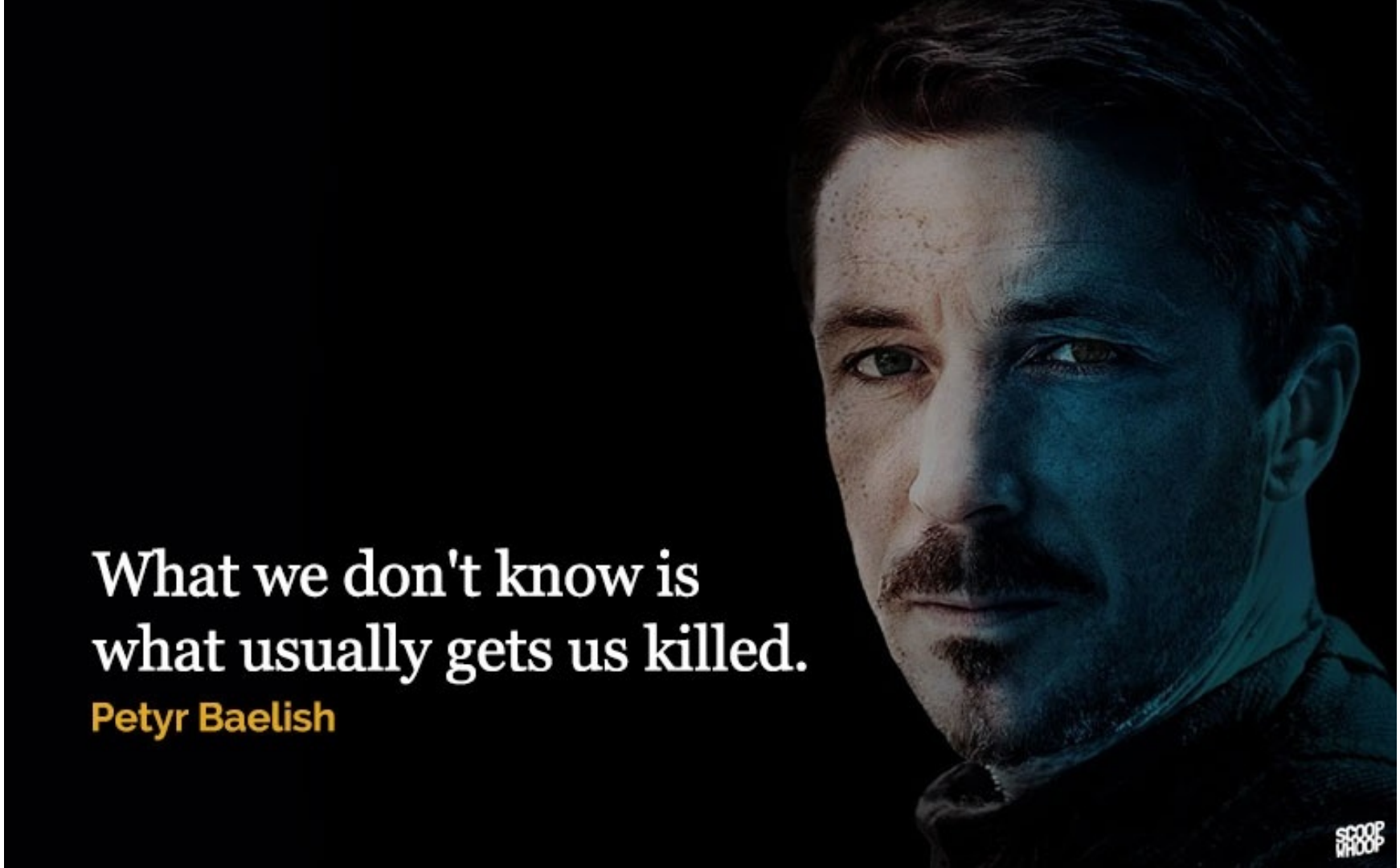
Pillars of Cyber-Risk Management

- Governance
- Risk Management
- Modernizing Technology
- Hardening Systems
- Cultural Change


*“To win Westeros,
you need support
from Westeros”*

Governance

- Establish Cyber-Risk Governance Committee
  - Cyber-Risk Responsible Executives (”Business”, not necessarily “technical”)
  - External Advisory Group
  - Internal Stakeholders– Line of business, Legal, Risk Services, Compliance and Audit, Procurement
  - Regular Face-to-Face meetings
  - Direct line of communication to highest levels of leadership
- Cyber-Risk Coordination Center
  - Programmatic arm of the committee
  - Does the “heavy lifting” of committee directives and recommendations


What we don't know is
what usually gets us killed.
Petyr Baelish

Risk Management

- **Principle-driven:** Agreement and adherence by all to core principles that drive our assessment of risk and actions to protect the institution(s)
- **Accountable:** Provides for tying actions to people and assigning necessary responsibility in a governance framework
- **Transparent:** Makes operations more auditable by increasing visibility into core processes, governance, and decision making
- **Measurable:** Provides the basis for continuous improvement and allows for the creation of a baseline that can be compared


Every
flight
begins
with a
fall

Modernizing Technology

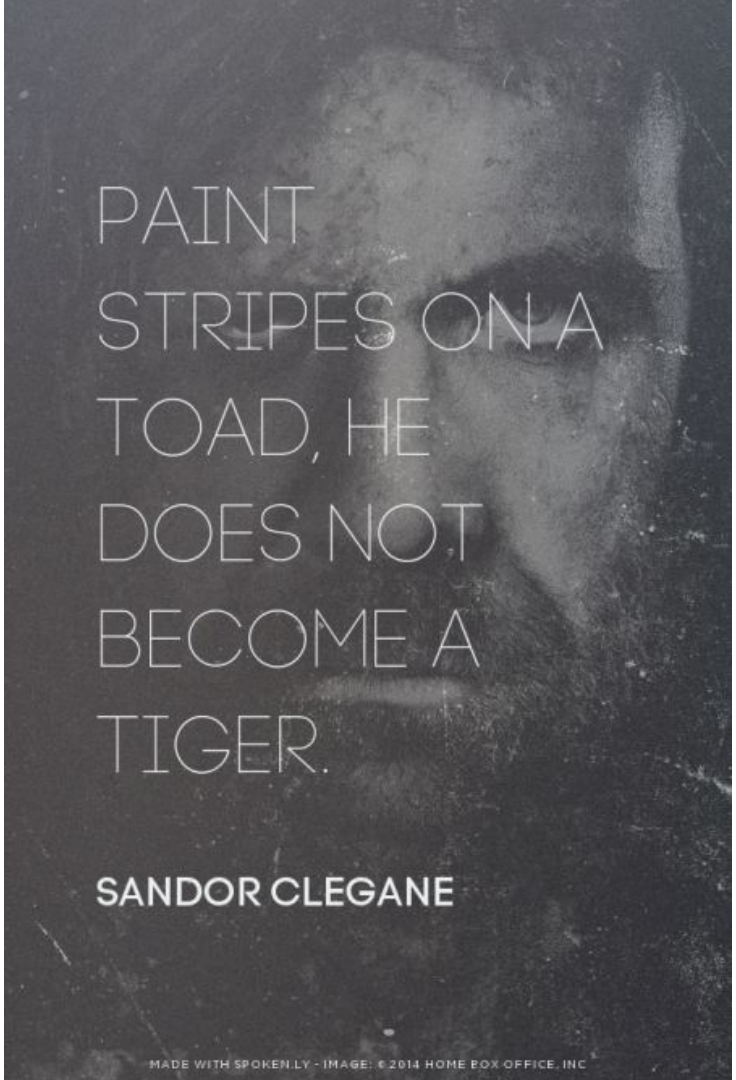
- Adoption of modern technology including execution of a plan at each location to upgrade technology and share best practices

- This will not only create consistency in cyber-defense approach but also leverages the investments that are being made across the organization


DIFFERENT ROADS
SOMETIMES LEAD TO
THE SAME CASTLE
- Jon Snow

Hardening Systems

- Coordinated threat intelligent information sharing across the organization, including outside sources
- Emphasis on best practices and protocols
  - Authentication, multi-factor
  - Patching
  - Vulnerability scanning, both platform and app
  - Penetration Testing


PAINT STRIPES ON A TOAD, HE DOES NOT BECOME A TIGER.
SANDOR CLEGANE
MADE WITH SPOKEN.LY - IMAGE: © 2014 HOME BOX OFFICE, INC

Cultural Change

- Focus on organizational cultural change
- Educating the workforce
- Enhancing security training of IT workforce
- Creation and execution of clear protocols of escalation


“
A bruise is a lesson...
and each lesson makes
us better.
– Arya Stark

Takeaways

- You don’t control the threat – You control your readiness
- Sustainable programs balance the need to protect against the need to achieve the mission
- Improve your resilience - protect, detect and respond
- Being consistent and coordinated is critical

RSAConference2018

#RSAC

THANK YOU!