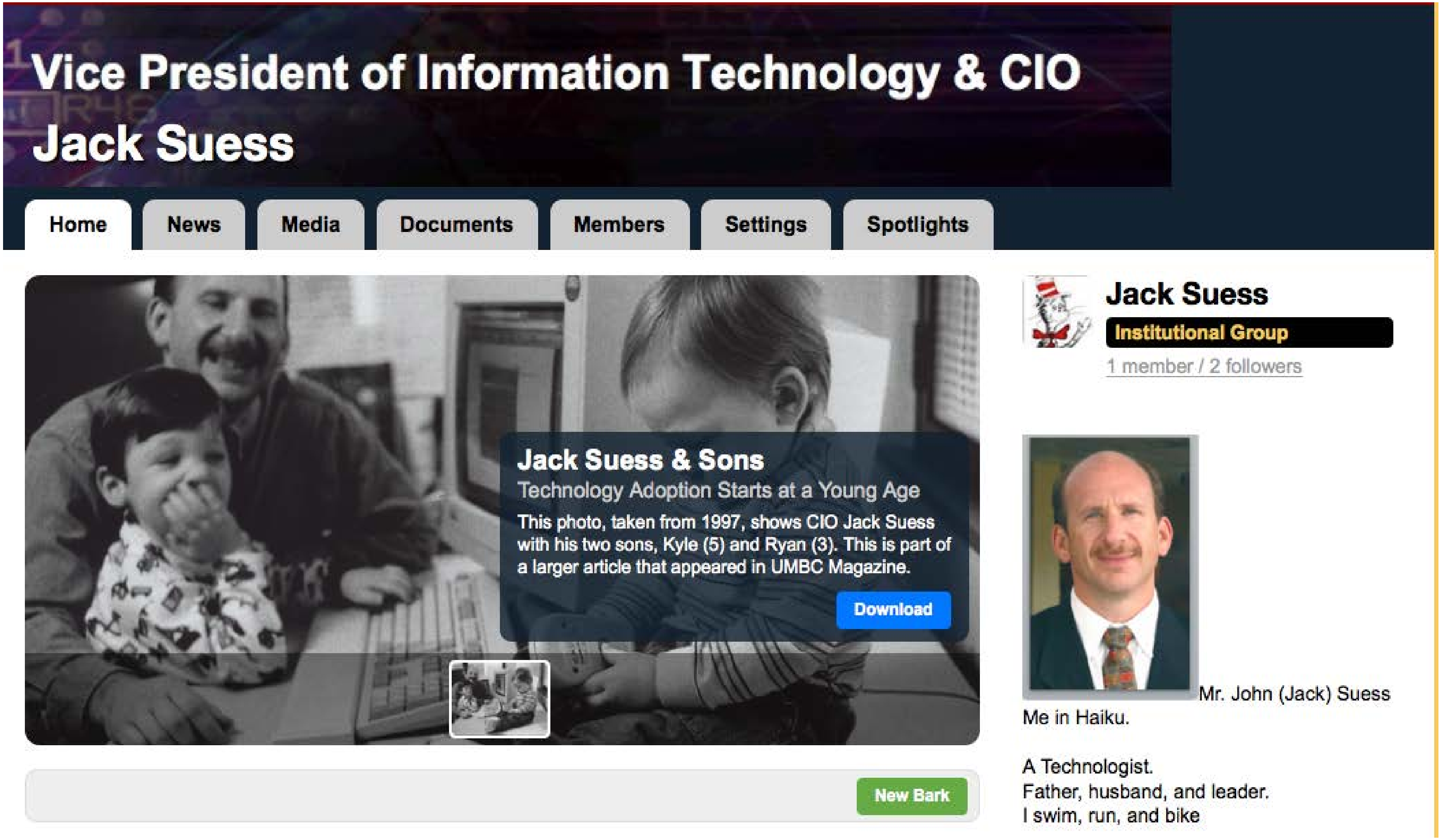
Empowering Our Organizational Culture to Meet Today's CyberSecurity Challenges

Jack Suess
Jack@umbc.edu



Vice President of Information Technology & CIO

Jack Suess

Jack Suess & Sons

Technology Adoption Starts at a Young Age

This photo, taken from 1997, shows CIO Jack Suess with his two sons, Kyle (5) and Ryan (3). This is part of a larger article that appeared in UMBC Magazine.

Jack Suess

1 member / 2 followers

Mr. John (Jack) Suess

Me in Haiku.

A Technologist.
Father, husband, and leader.
I swim, run, and bike

http://my.umbc.edu/groups/jack

George Santayana (1863-1952)

"Habbit is stronger than reason."

"Those that do not learn from history are doomed to repeat it."

"Wisdom comes from disillusionment."

Stand if you feel cybersecurity is important to your organizations mission.

Keep standing if you feel everyone else in your organization views cybersecurity as importantly as you do to your organization's success.

Keep standing if you feel your present approach to cybersecurity is certain of achieving success.

Empowering Our
Organizational Culture to
Meet our CyberSecurity Challenges

Why Rethink Our Approach to Cybersecurity?

It isn't **WORKING**!!

Why Do I Claim Is Not Working

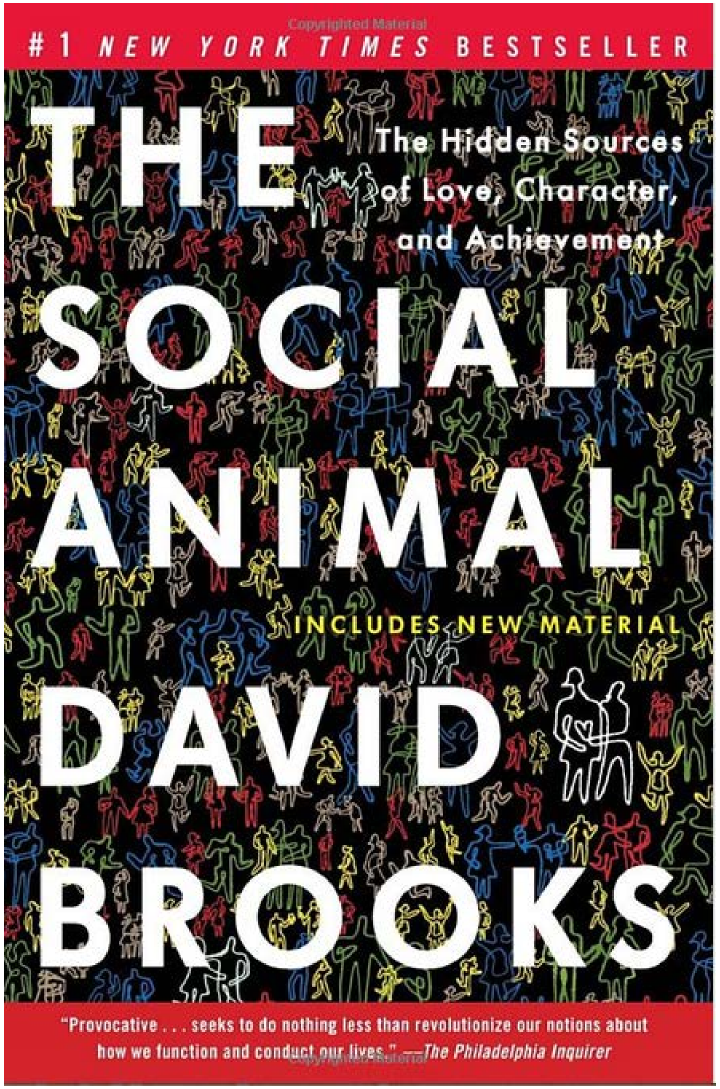
- Do we see any evidence that the quantity of cybersecurity issues are decreasing?
- Do we see any evidence that impact from cybersecurity events are decreasing?
- Do we see any evidence that there will soon be a major technological breakthrough that will make cybersecurity less daunting for organizations?

Why isn't it working? People!

George Santayana (1863-1952)

"Habbit is stronger than reason."

The Challenge of Culture



Copyrighted Material
#1 NEW YORK TIMES BESTSELLER
THE SOCIAL ANIMAL
The Hidden Sources of Love, Character, and Achievement
INCLUDES NEW MATERIAL
DAVID BROOKS
"Provocative . . . seeks to do nothing less than revolutionize our notions about how we function and conduct our lives." —The Philadelphia Inquirer
Copyrighted Material

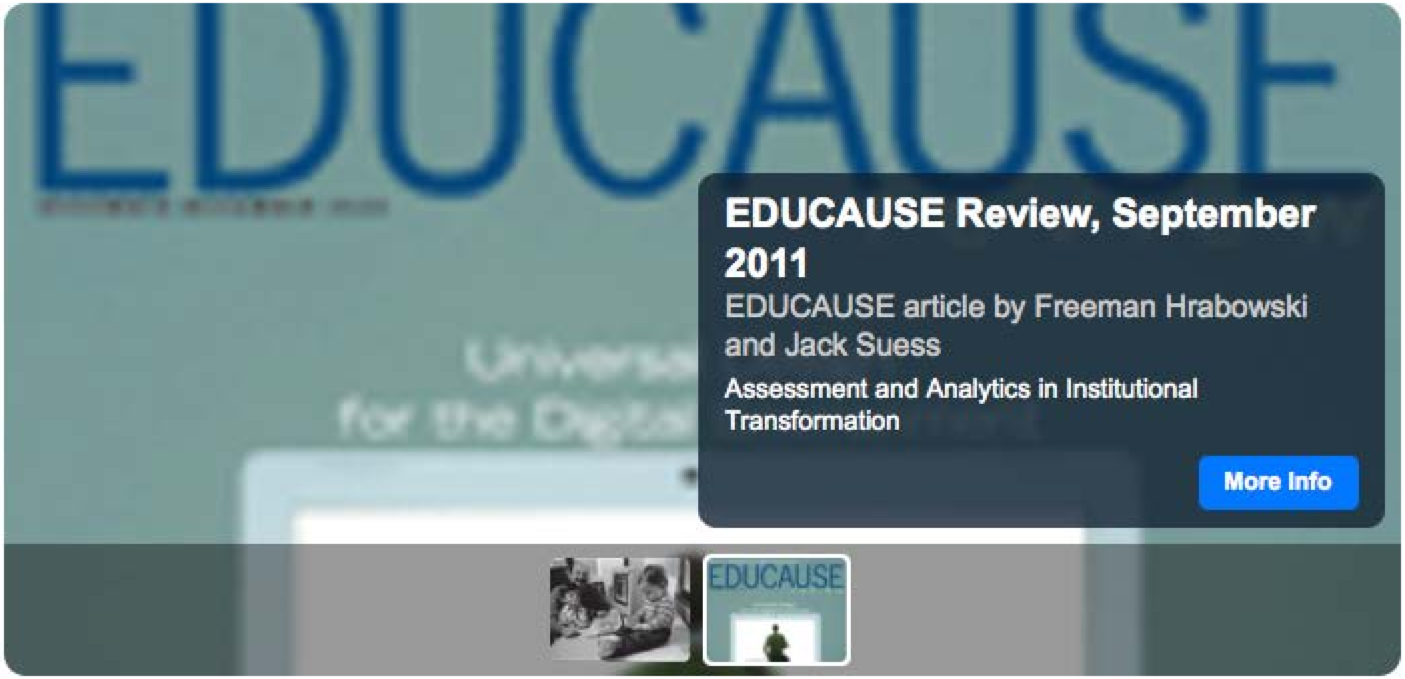
- Culture is informed by and helps create our habits, beliefs, practices, and relationships.
- This culture drives individuals to become accustomed to performing duties in a set way.
- Any major change in what people do requires convincing people to change.

Organization Culture

-- noun

The customs, rituals, and values shared by the members of an organization that have to be accepted by new members.

Role of Culture in Instituitional Transformation



EDUCAUSE Review, September 2011

EDUCAUSE article by Freeman Hrabowski and Jack Suess

Assessment and Analytics in Institutional Transformation

What Are Some of the Problems UMBC Has Changed the Culture On?

- Minority achievement, especially in Science, technology, engineering, and math (STEM)

- Graduate education, especially Ph.D. completion.
- Faculty pedagogy and teaching.
- Financial controls and auditing.

UMBC Lessons Learned

1. Leadership matters.
2. It is a institution-wide effort.
3. It requires a holistic approach that needs to be tailored for different stakeholder groups.
4. There is a financial commitment we must make if we want to succeed.
5. Professional development is essential.
6. Recognition and rewards are important
7. Remember

Success is never final!

I Know What You Are All Saying

Minority Achievement,

Ph.D. Completion,

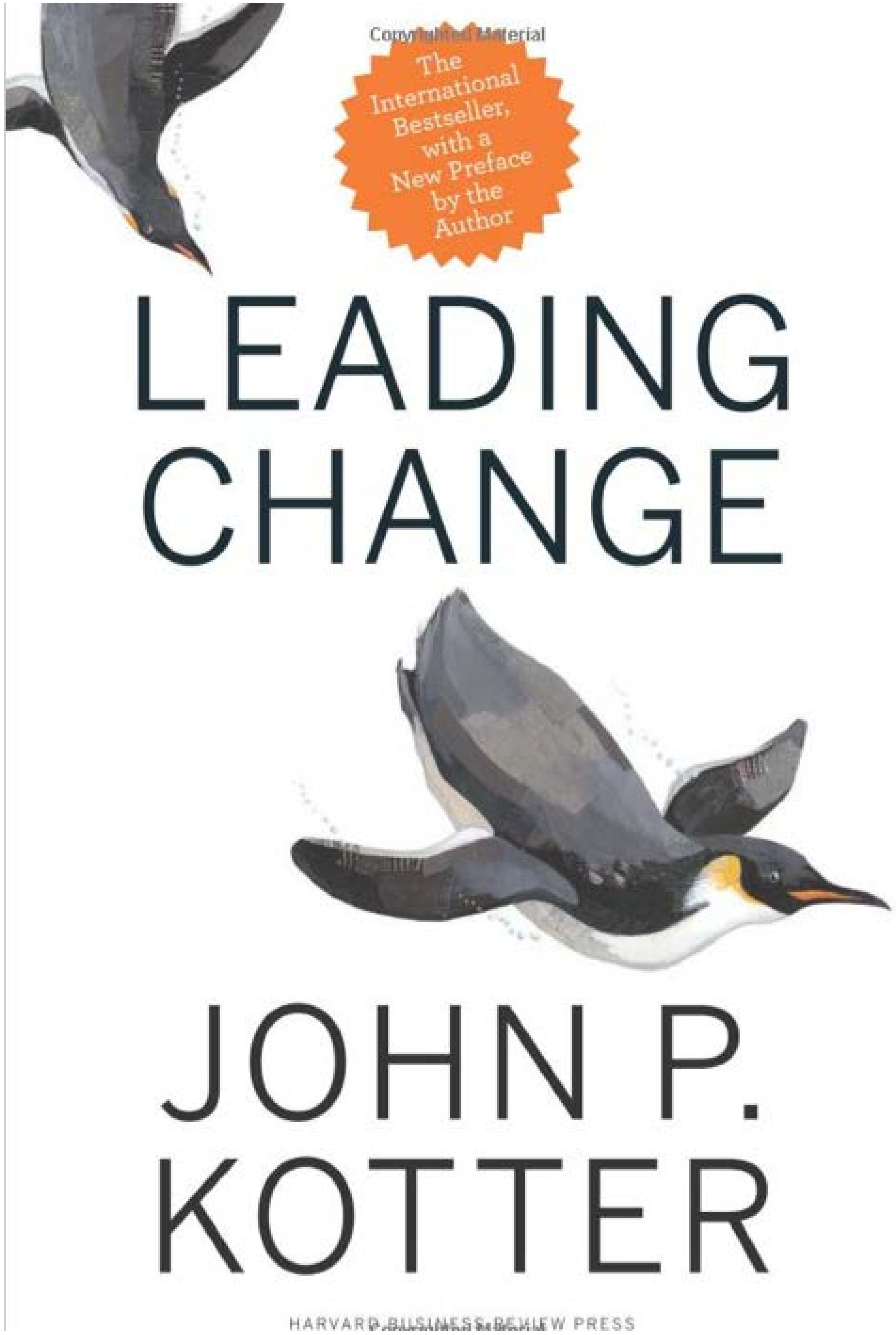
Getting Faculty to Change,

These Are Easy

Cybersecurity is **hard**, its **technical**, people are even **attacking you**!

How do these lessons apply?

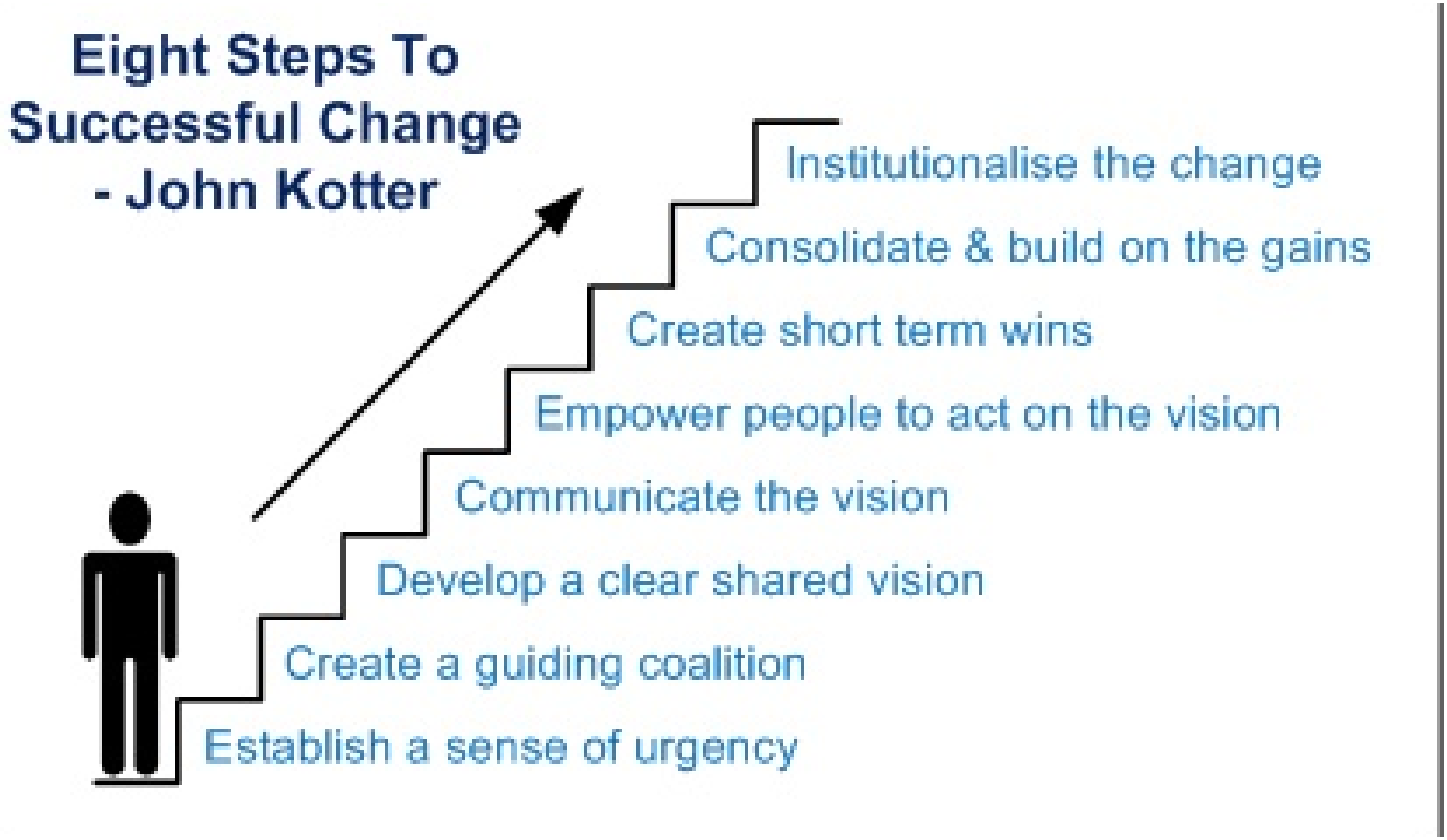
Tough Problems Require People to Change


Copyrighted Material
The International Bestseller, with a New Preface by the Author
LEADING CHANGE
JOHN P. KOTTER
HARVARD BUSINESS REVIEW PRESS

The Seminal Work on Change

John P. Kotter

Kotter's Eight Steps for Change



Eight Steps To
Successful Change
- John Kotter

Institutionalise the change

Consolidate & build on the gains

Create short term wins

Empower people to act on the vision

Communicate the vision

Develop a clear shared vision

Create a guiding coalition

Establish a sense of urgency

Leaders Establish a Sense of Urgency

Why Change? What's in it for me?

Leaders relate why change is necessary. Without people believing that change is necessary they will revert to their habits.

How does it apply to cybersecurity?

For UMBC - its about **Mission & Values.**

Cybersecurity drives economic development, jobs for students, research for faculty, it protects our community's privacy, & ensures we are good stewards of state resources.

Leaders Create a Guiding Coalition

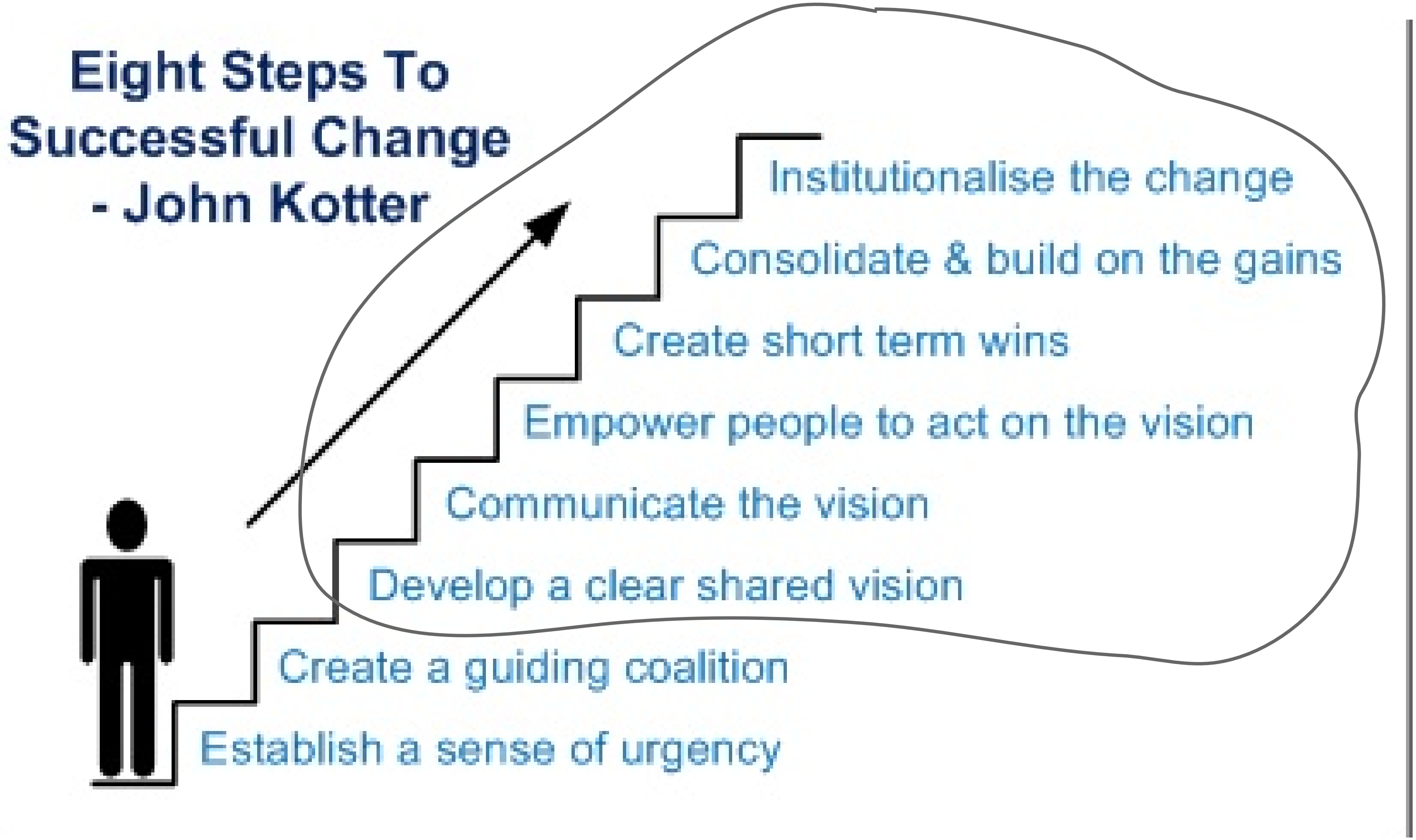
Who is part of this coalition?

Key leaders, people with **expertise**, people with organizational **credibility**, and members of CEO's team. This group **develops** and **executes** the vision and plan.

Applicability to Cybersecurity

Must be more than IT and needs to leverage skills in communication, marketing, academic expertise to create a deep and broad plan to carry out Kotter's six remaining steps.

Planning and Executing Change



Eight Steps To Successful Change - John Kotter

Institutionalise the change

Consolidate & build on the gains

Create short term wins

Empower people to act on the vision

Communicate the vision

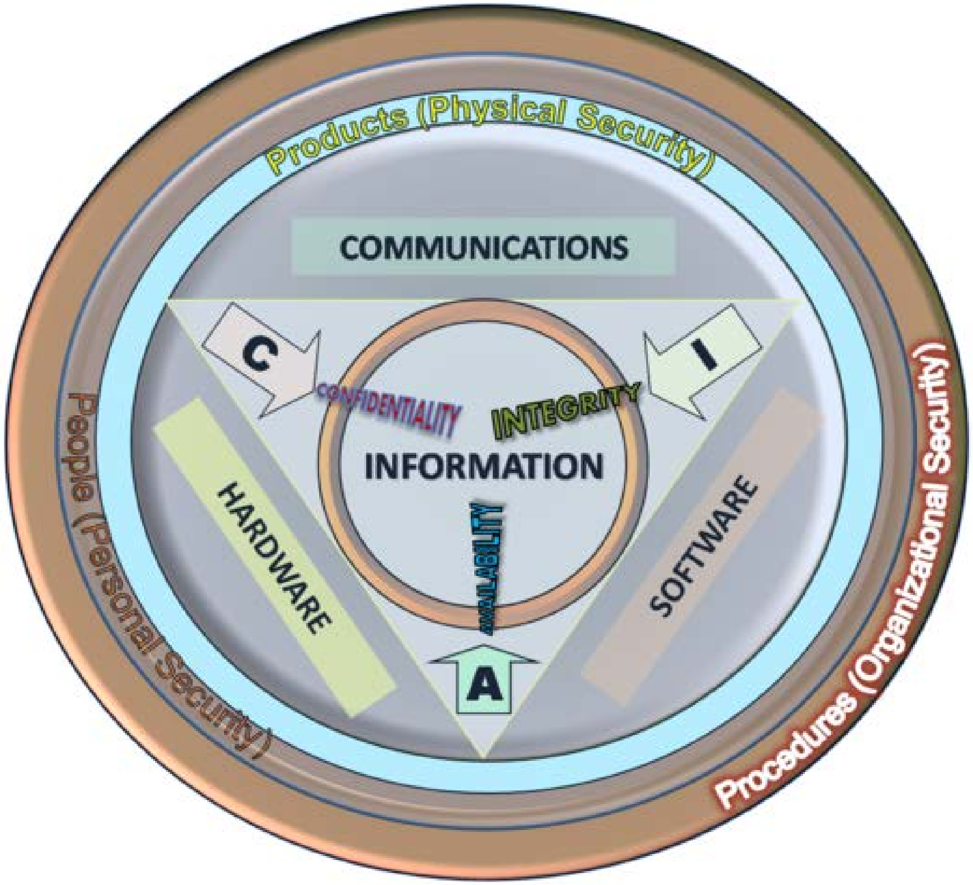
Develop a clear shared vision

Create a guiding coalition

Establish a sense of urgency

Communication and Vision

Is this our shared vision for cybersecurity? **ConfidentialityIntegrityAvailability**



Products (Physical Security)
COMMUNICATIONS
C
I
CONFIDENTIALITY
INTEGRITY
INFORMATION
AVAILABILITY
HARDWARE
SOFTWARE
A
People (Personal Security)
Procedures (Organizational Security)

My Vision for UMBC Cybersecurity

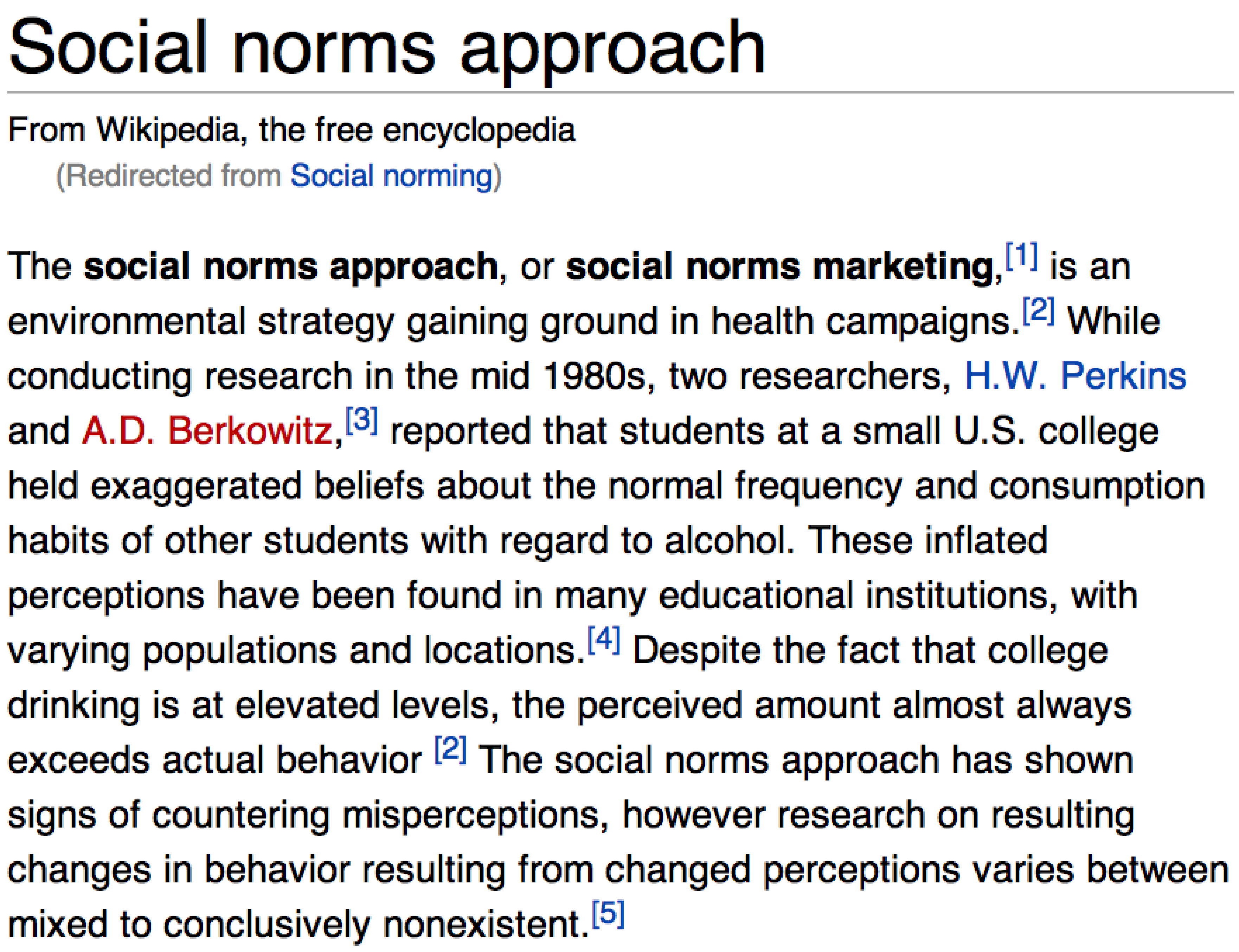
Through **teaching**, **scholarship**, and **innovative** use of technology, UMBC will **empower** faculty, staff, and students with the **skills** and **resources** necessary to **safeguard** our **digital assets** and **protect** their **privacy** and that of the other members of our community.

Communication and Marketing

- We can't over-communicate vision and goals. Does October as cyber security awareness month cut it? Lets have **no-PHISH Fridays** every week**!**
- Tailoring the message to the audience is critical. **Storytelling is very powerful**.
- Communication is as much about actions as it is words. Lead by example and walk the talk.
- Assess impact, refine message, assess again - BUT KEEP Communicating.

Anonymous Audience Response

These are a great way to get quick and honest feedback to break the ice and understand culture in different groups.



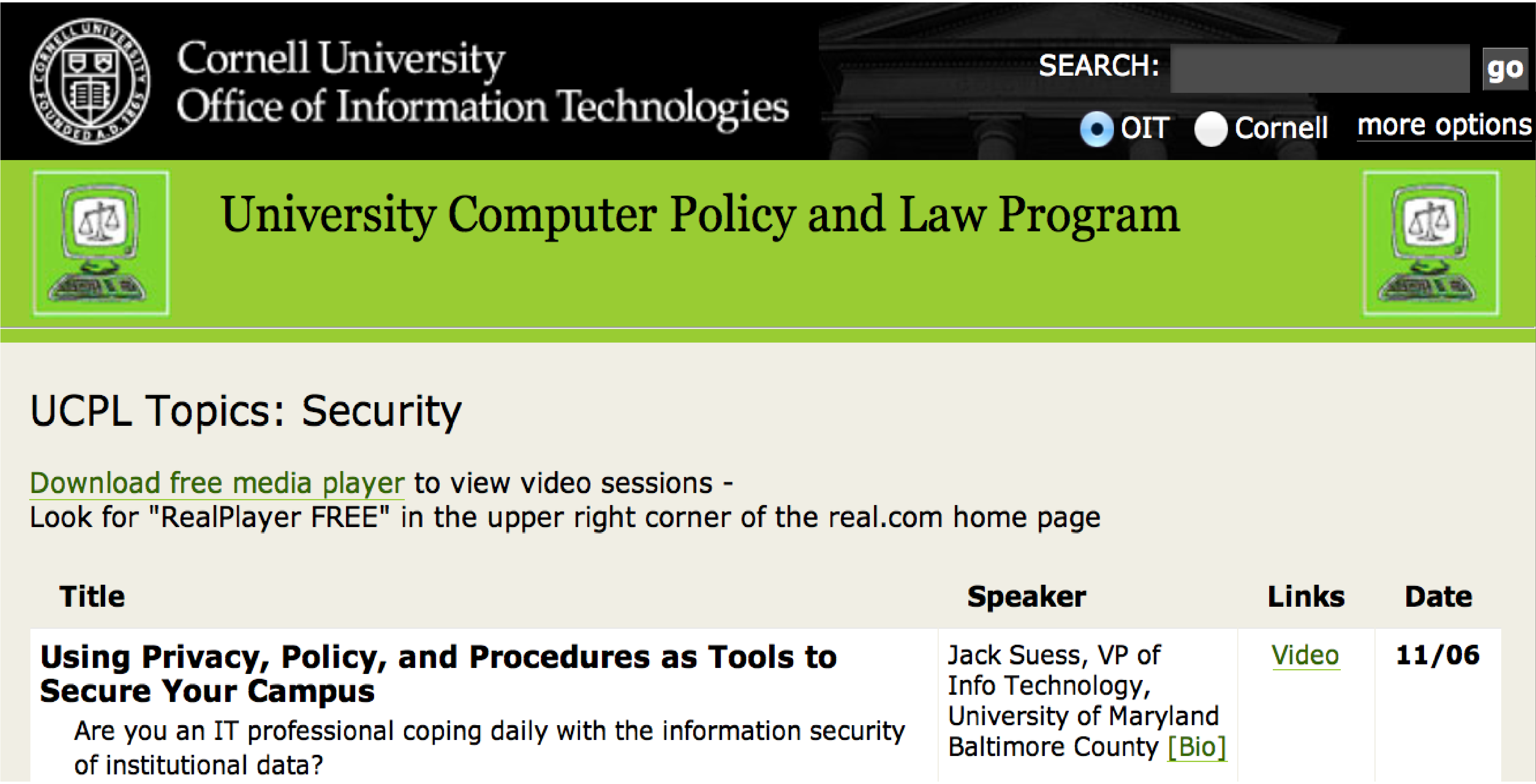
Social norms approach

From Wikipedia, the free encyclopedia

(Redirected from Social norming)

The **social norms approach**, or **social norms marketing**,[1] is an environmental strategy gaining ground in health campaigns.[2] While conducting research in the mid 1980s, two researchers, H.W. Perkins and A.D. Berkowitz,[3] reported that students at a small U.S. college held exaggerated beliefs about the normal frequency and consumption habits of other students with regard to alcohol. These inflated perceptions have been found in many educational institutions, with varying populations and locations.[4] Despite the fact that college drinking is at elevated levels, the perceived amount almost always exceeds actual behavior [2] The social norms approach has shown signs of countering misperceptions, however research on resulting changes in behavior resulting from changed perceptions varies between mixed to conclusively nonexistent.[5]

Privacy as the Key to Security



Cornell University
Office of Information Technologies

University Computer Policy and Law Program

UCPL Topics: Security

Download free media player to view video sessions -
Look for "RealPlayer FREE" in the upper right corner of the real.com home page

Title	Speaker	Links	Date
Using Privacy, Policy, and Procedures as Tools to Secure Your Campus Are you an IT professional coping daily with the information security of institutional data?	Jack Suess, VP of Info Technology, University of Maryland Baltimore County [Bio]	Video	**11/06**

Why Privacy and Not Security

- People **care** about their **privacy** and that of their colleagues. This helps create a sense of urgency.
- People use technology at home and want to protect their own personal privacy.
- Mass communication focuses on the threat to privacy. People are scared and will listen.
- Good work environments focus on community building, this strengthens that.

Applying Communcation Lessons to Cybersecurity

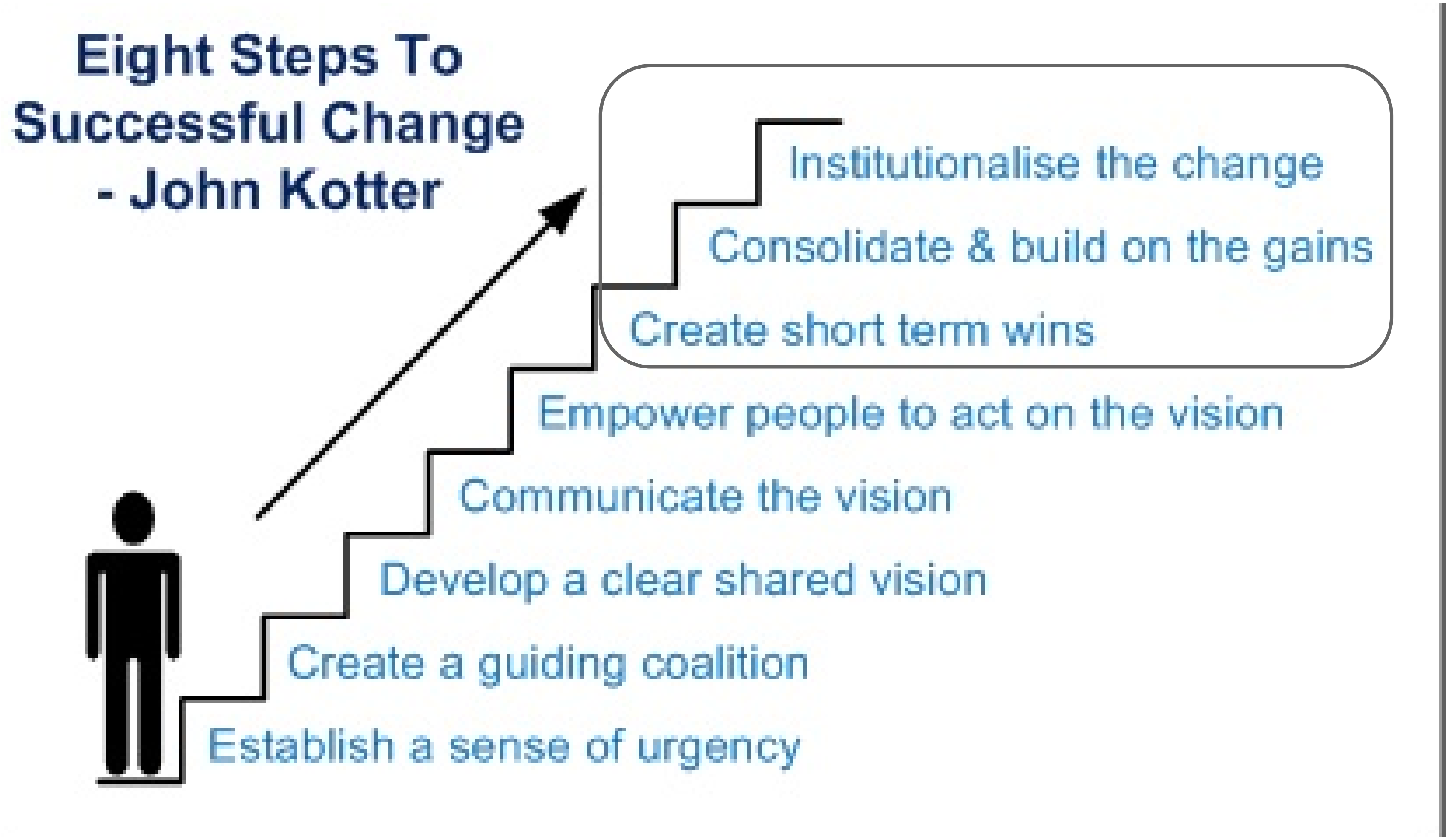
- Connect cybersecurity to your mission and regularly communicate your vision.
- Consider adding a focus on privacy.
- Develop success stories or stories of loss that can connect with audiences.
- Regularly survey stakeholders.
- Use social norming techniques to show that people can change and that some behaviors are not as common as thought.
- Have fun!

Passwords are like underwear...
Change yours often.

Passwords are like underwear... Don't share them with friends

Passwords are like underwear... Be mysterious.

Changing Culture is a Long-Term Committment



Eight Steps To Successful Change - John Kotter

Institutionalise the change

Consolidate & build on the gains

Create short term wins

Empower people to act on the vision

Communicate the vision

Develop a clear shared vision

Create a guiding coalition

Establish a sense of urgency

This is a Long-Term Effort

- You need small wins along the way to show you are making progress and maintain the commitment of people.
- Often large scale change requires new approaches to the problem.
- Institutionalizing the change means you have created a new culture, that usually takes **years** to happen.

This is why leadership must be committed and this effort tied to mission & values.

Long-Term Implications for an Organization's Cybersecurity

I feel we will have success when

- Our leaders regularly talk about how far we have come and how far we need to go.
- Our organizational development strategy includes a focus on cybersecurity.
- Management training includes modules on cybersecurity and privacy.
- In their annual performance review, everyone is evaluated on their efforts to protect privacy.
- Technology innovates and experiments to

Imagine

An organization where all individuals are encouraged and supported to take ownership for protecting the privacy of the community, are proactive in supporting their colleagues professional development, and work to identify new ways to improve cybersecurity readiness in support of our mission.

This is where I want to work!

Implications for Technology & Support

George Santayana (1863-1952)

"Those that do not learn from history are doomed to repeat it."

Monterey, California

THESIS

SUBVERSION:

THE NEGLECTED ASPECT OF COMPUTER SECURITY

by

Philip A. Myers

June, 1980

Morris Worm - November 2, 1988

Robert Morris

Refer to [RFC 1135]

If what we were doing in technology was working, wouldn't we have seen the results by now?

Technology Organizations Must Change Our Approach as Well

- Work with leaders to understand and manage risk.
- Developing policies and procedures that can be understood and accommodate the reality of work.
- Encourage your team to be creative and innovative in identifying solutions.
- Emphasize a culture of data classification, protection, and privacy.
- Make certain everyone in IT can securely do their job

Managing and Communicating Risk

- Managing risk is the essential element of UMBC's strategy.
- Risk is all about data protection!
  - Risk is tied tightly to data classification or regulatory requirements.
  - Every technical member of the staff has been trained on our risk process and knows they are accountable for letting management know of risk factors.
- Senior IT management annually reviews all risk mitigation and management plans.

Data Classification, Protection, and Privacy

- **Privacy protection** drives our data classification strategy. Protecting the education, financial, and health records is **our responsibility** to our community.
- Data stewards dealing with these records feel they have an **obligation** to our community to take steps to protect data.
- **Data classification drives** our risk management process.
- **Risk** management drives **security requirements**

Policies and Procedures

- Internally for IT, procedures are essential. Without documentation it is too easy to make a configuration mistake that would create a security vulnerability.
- Policies must be understandable and implementable. Too often IT policies are not understandable or we have thought through how users can implement them.
  - Bad policies are WORSE than no policies.

Creativity and Innovation

IT people are natural problem solvers.

- Challenge your staff's creativity to find solutions to vexing problems
  - Phishing case study.
- Leverage your broader community in sharing information and resources.
  - REN-ISAC case study

IT Professionals & Security

- We should never assume that IT professionals understand security or our trained to do their job securely.
- Every IT professional should have a professional development plan that includes cybersecurity.
- Security must be owned by everyone, not just the CISO.
- Procedures and accountability are essential.

Where Does This Leave Us

George Santayana (1863-1952)

"Wisdom comes from disillusionment."

policy@edu

By Joy R. Hughes and Jack Suess

Presidents and Campus Cybersecurity

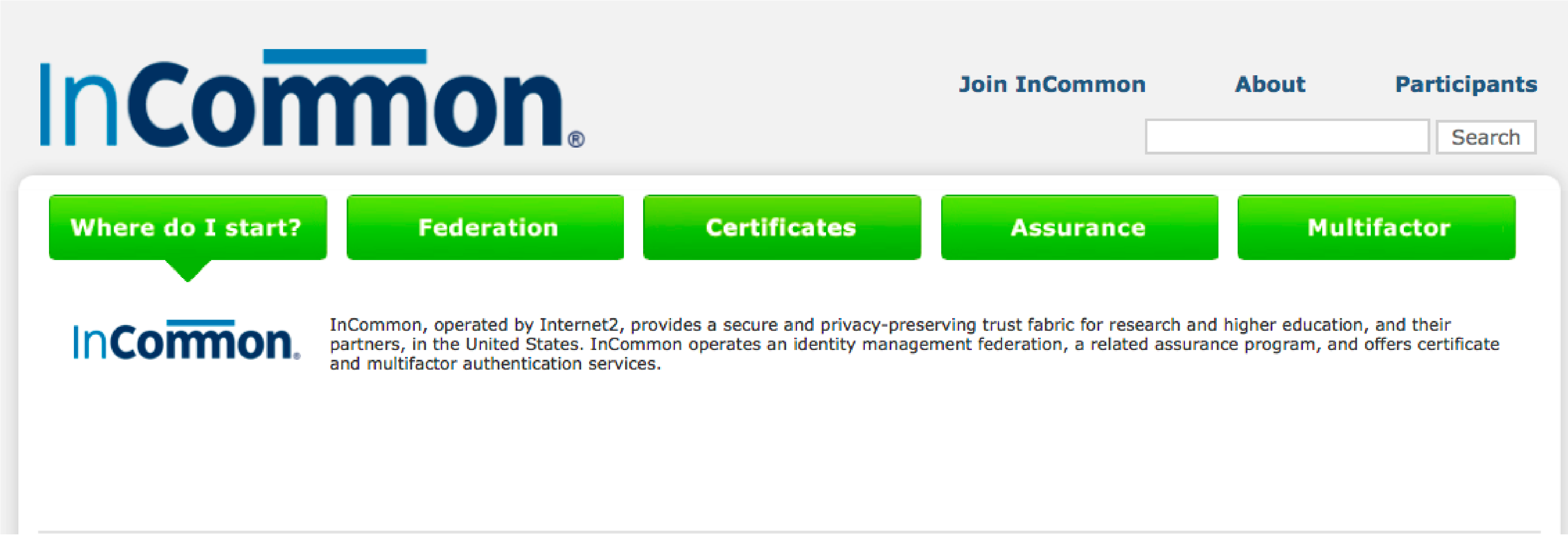
CIOs cringe when they hear about the latest security incident at some other college or university. They know that their colleagues at the other institution are being besieged by anxious students, parents, alumni, faculty, and staff—all of whom are angry that the institution has betrayed their trust by allowing access to private data. The CIOs know that the federal agencies that provide research dollars to the institution will be calling to find out if research data were at risk and may lose confidence in the institution's ability to protect that data. They know that if the college or university is a state institution, there is bound to be a resolution (or two) introduced in the state legislature to allow greater control of the institution's IT systems. They also know that the same security problem that led to the reputation-harming press coverage for the compromised institution exists on their own campuses. Even though their own campuses may not have suffered a major infiltration by a criminal or mali-

detection and protection systems in order to keep them that way. In addition, at most institutions, many of the servers, desktops, and laptops that store private data are not under the control of the campus CIO. The data on these machines often come directly from the central administrative systems.

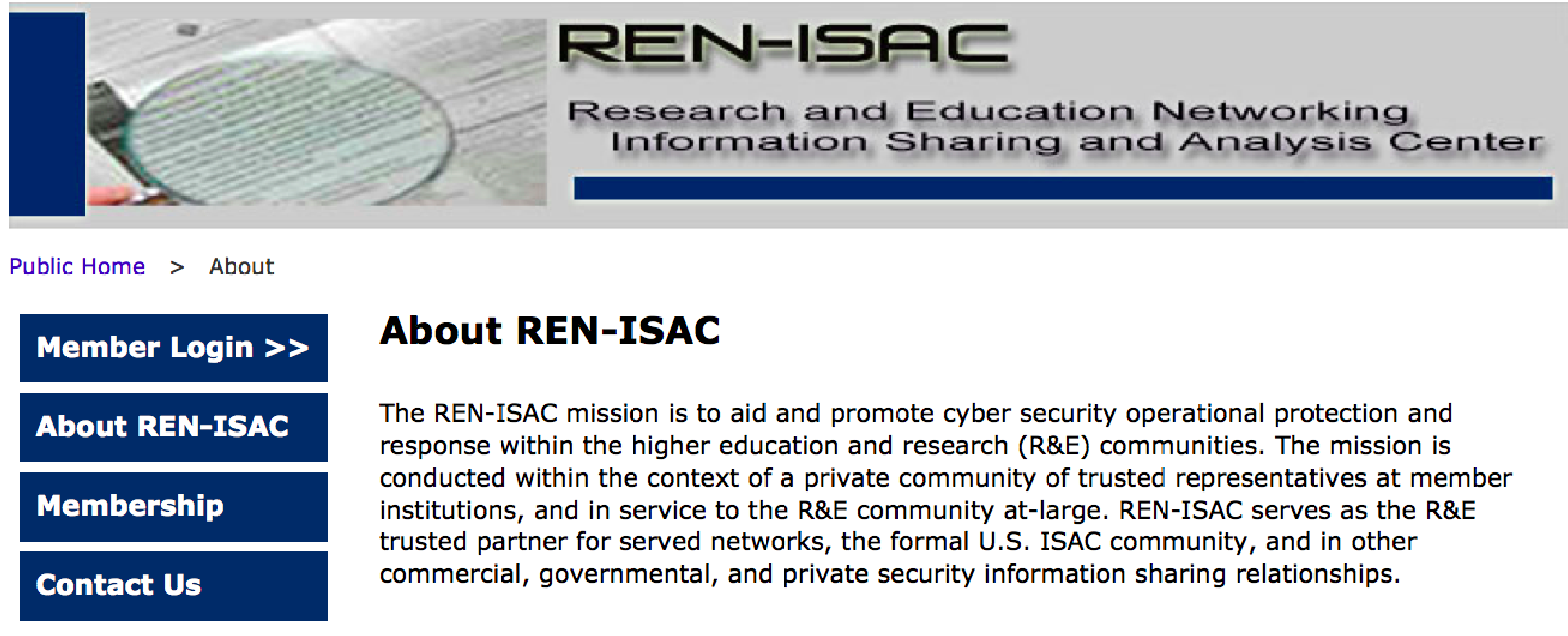
The campus meal plan server, the housing server, the parking services server, the campus police server, and the international students office server are examples of servers that store confidential data, that are not usually managed by central IT, and that have been hit by hackers in highly publicized incidents. Often, the people administering these servers wear many hats and do not have the time or the expertise to keep the servers secure. The hardware may be old and the operating systems too outdated to be made secure.

Higher education institutions expend enormous effort and money to secure central systems, but then they allow departments and individuals to download

UC-Berkeley would do all that it could to safeguard personal data stored on campus computers. He wrote: "As Chancellor of the Berkeley campus, I was stunned to learn of the theft of a laptop computer in the Graduate Division, which contained personal information for approximately 98,000 current and former graduate students as well as persons who applied to our graduate programs. Our students, staff and alumni expect us to protect the information they have given us confidentially, and we have not maintained that trust. This incident revealed serious gaps in our management of this kind of data. The campus has been instituting new policies to address these issues for several months, and we will do much more. Accountability for this effort ultimately lies with me." Birgeneau promised to "engage one of the nation's leading data-security management firms to conduct an immediate external audit of how the campus handles all personal information. This firm will examine the security of the systems, the policies and practices regarding

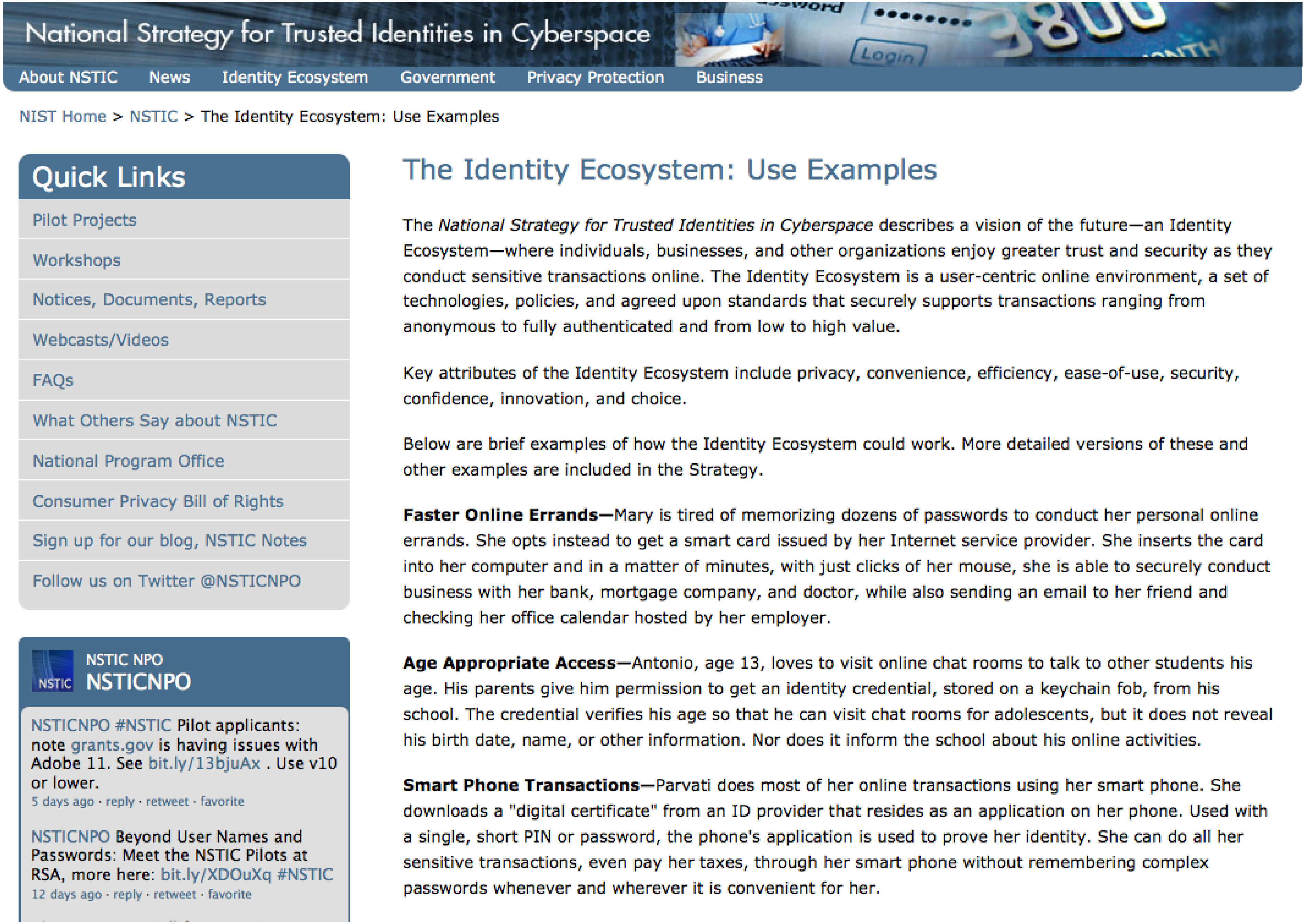


InCommon, operated by Internet2, provides a secure and privacy-preserving trust fabric for research and higher education, and their partners, in the United States. InCommon operates an identity management federation, a related assurance program, and offers certificate and multifactor authentication services.



About REN-ISAC

The REN-ISAC mission is to aid and promote cyber security operational protection and response within the higher education and research (R&E) communities. The mission is conducted within the context of a private community of trusted representatives at member institutions, and in service to the R&E community at-large. REN-ISAC serves as the R&E trusted partner for served networks, the formal U.S. ISAC community, and in other commercial, governmental, and private security information sharing relationships.



National Strategy for Trusted Identities in Cyberspace

About NSTIC News Identity Ecosystem Government Privacy Protection Business

NIST Home > NSTIC > The Identity Ecosystem: Use Examples

Quick Links

- Pilot Projects
- Workshops
- Notices, Documents, Reports
- Webcasts/Videos
- FAQs
- What Others Say about NSTIC
- National Program Office
- Consumer Privacy Bill of Rights
- Sign up for our blog, NSTIC Notes
- Follow us on Twitter @NSTICNPO

NSTIC NPO
NSTICNPO

NSTICNPO #NSTIC Pilot applicants: note grants.gov is having issues with Adobe 11. See bit.ly/13bjuAx . Use v10 or lower.
5 days ago · reply · retweet · favorite

NSTICNPO Beyond User Names and Passwords: Meet the NSTIC Pilots at RSA, more here: bit.ly/XDOuXq #NSTIC
12 days ago · reply · retweet · favorite

The Identity Ecosystem: Use Examples

The *National Strategy for Trusted Identities in Cyberspace* describes a vision of the future—an Identity Ecosystem—where individuals, businesses, and other organizations enjoy greater trust and security as they conduct sensitive transactions online. The Identity Ecosystem is a user-centric online environment, a set of technologies, policies, and agreed upon standards that securely supports transactions ranging from anonymous to fully authenticated and from low to high value.

Key attributes of the Identity Ecosystem include privacy, convenience, efficiency, ease-of-use, security, confidence, innovation, and choice.

Below are brief examples of how the Identity Ecosystem could work. More detailed versions of these and other examples are included in the Strategy.

Faster Online Errands—Mary is tired of memorizing dozens of passwords to conduct her personal online errands. She opts instead to get a smart card issued by her Internet service provider. She inserts the card into her computer and in a matter of minutes, with just clicks of her mouse, she is able to securely conduct business with her bank, mortgage company, and doctor, while also sending an email to her friend and checking her office calendar hosted by her employer.

Age Appropriate Access—Antonio, age 13, loves to visit online chat rooms to talk to other students his age. His parents give him permission to get an identity credential, stored on a keychain fob, from his school. The credential verifies his age so that he can visit chat rooms for adolescents, but it does not reveal his birth date, name, or other information. Nor does it inform the school about his online activities.

Smart Phone Transactions—Parvati does most of her online transactions using her smart phone. She downloads a "digital certificate" from an ID provider that resides as an application on her phone. Used with a single, short PIN or password, the phone's application is used to prove her identity. She can do all her sensitive transactions, even pay her taxes, through her smart phone without remembering complex passwords whenever and wherever it is convenient for her.

My Recomendations

"Habbit is stronger than reason."

- We must focus on changing our organizational culture around cybersecurity.

"Those that do not learn from history are doomed to repeat it."

- IT organizations must adapt and innovate to meet the cybersecurity challenge.

"Wisdom comes from disillusionment."

- Cybersecurity is now a long-term issue and success is never final!

Hope Springs Eternal!

I'm optimistic for these reasons:

- We recognize we have a long-term problem and we are committing significantly more resources to address the problem.
- Our leaders are recognizing that this is a societal issue and not just an IT issue.
- We are looking at innovative approaches to rethink cybersecurity.
- We have people like yourselves that are working to change our culture!

Thank You!

Jack Suess
Jack@umbc.edu
http://my.umbc.edu/groups/jack

Cybersecurity has often been viewed as an IT initiative and is often focused narrowly on a small percentage of the individuals In an organization. As new threats emerge, such as social engineering, to broadly target individuals we need new approaches to address the challenge of cybersecurity. Broadly speaking, we need an approach that looks at cybersecurity holistically and builds support for a multi-year approach that incorporates better technology, new business processes, and an emphasis on communicating and educating workers. This approach requires leadership commitment to a long-term strategy for change management and organizational development around cybersecurity.

This talk will focus on ideas for effective change management and organizational development that are coupled with strategies for cybersecurity education, information sharing, and support to create long-term success. The talk will look at approaches used in other fields to change behavior and beliefs that could be used as models to build support for the change necessary to dramatically improve cybersecurity in our organizations. I will draw on approaches being developed in the higher education sector as well as lessons learned that can be applied to other groups.