

# Sense and Reliability:

*Do we have the right approach to risk management for our future – especially when it comes to cybersecurity?*

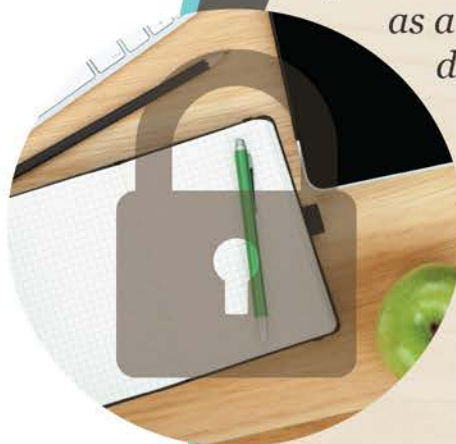
---

---

October 2015

*“Balance is key - cyber risk needs to be managed; it can’t be eliminated. Once you realize you can’t eliminate it, everything else can be classified, prioritized, and dealt with as a rational business decision.”*

*Matt Sawtell  
CU\*Answers  
Assistant VP of  
Managed  
Technology*



## **About CU\*Answers, Inc.**

CU\*Answers offers expertise in implementing technical solutions to operational needs, and is a leader in helping credit unions form strategic alliances and partnerships.

CU\*Answers provides a wide variety of services for credit unions including its flagship CU\*BASE® processing system (online and in-house) and Internet development services featuring **It's Me 247** online and mobile banking. Additional services include web development, network design and security, and image check processing. Founded 40+ years ago, CU\*Answers is a 100% credit union-owned cooperative CUSO providing services to credit unions representing over 1.8 million members and \$17 billion in credit union assets. For more information, visit [www.cuanswers.com](http://www.cuanswers.com).

## Sense and Reliability:

# Do we have the right approach to risk management for our future – especially when it comes to cybersecurity?

*Randy Karnes, CU\*Answers, CEO*

Give this article a read: <https://hbr.org/2003/04/sense-and-reliability> (“Sense and Reliability” by Diane Coutu, published in the April 2003 issue of the Harvard Business Review.)

*A copy of this article is included beginning on Page 23.*

I like these ideas and wonder how we might be a HRO (High Reliability Organization) for our clients. Are we? How do we test the perception of our marketplace?

Do we have the right sense of “mindfulness” about their risks (fraud, regulatory, cybersecurity)? Do we have the power to detect and act on even weak signals of impending danger?

Based on our modeling for our marketplace and our goals for credit union sustainability can we blend our talents to make sure that we are not alarmists who put people and organizations on a track to exit businesses, based on fears that we identify?



# What It Means to be a Highly Reliable Organization

*Jim Lawrence, Manager, Business Continuity and Recovery Services / CBCP*

## Cybersecurity

Before I share my thoughts on what CU\*Answers can learn from HROs and becoming more mindful, let me start with cybersecurity as it relates to business resilience. This is a huge opportunity for us to serve our clients and participate in their success by helping them navigate the changing environment they operate in (rather than seeing this solely as a revenue stream). In fact in some ways, we're already responding to the call.

Below are just a few of the slides from the Cybersecurity presentation I gave in New Orleans. In the 90-minutes I was given, I attempted to help the credit unions who attended to filter through the mass of information that's thrown at them and to see through the hype generated by opportunistic vendors (and some regulators). My goal was to give them a clearer understanding in their own language that goes beyond the definitions and statistics to identifying actions they can take today to determine where they are now, set an obtainable target, and begin taking steps in that direction.

In slide #7 below I include a statement in a PwC publication (*Cyber: Think Risk, not IT*) that says "Despite millions of dollars spent on enhancements, cybersecurity remains the area of risk management with the largest gap between threat and preparedness." I feel strongly that one of the key reasons for the gap stems from a lack of clarity and understanding of the threat and potential impact on the organization. It's still being treated as a technology issue and in many cases outsourced to a dangerous level. Partnering with a vendor to gain the skills, experience, and tools required is strongly recommended, but the task of managing the risk is still on the organization (in this case the credit union). We should respond to the (over-worked and under-resourced) CEO that says "can't you just do it for me" with a convincing reason and solution that accomplishes the goal "with them not for them". The language we use to describe how risk is managed (including cyber risk) should be compatible with their operations.

I believe that more education needs to be provided for credit unions and more feedback from the credit unions. I would be more than happy to assist in this, working with the rest of the team (Dave Wordhouse, Patrick Sickels, Jim Vilker, Matt Sawtell, etc.). In addition to education, affordable solutions need to be provided to fill the job they're looking to hire (across all layers of risk management). I see these coming together across multiple teams and brands in 2016.

## High Reliability Organizing

I enjoyed reading the link you provided. I've been a subscriber to HBR.org for the past few years and have a number of favorite authors who post regularly.

I had not heard of the term HRO prior to this article. I found the content intriguing enough to pursue researching some of the cited resources including: *“Managing the Unexpected”* by Weick and Sutcliffe and *“Managing the Unexpected by Building up Organizational Capabilities”* by Gebauer and Kiel-Dixon.

Your comments during the Capacity Planning meeting last Thursday made me dig a little deeper into this article to learn how an HRO would think about them. You stated that “we are very good at responding to things that break. We drop what we’re doing and attack the issue from multiple fronts. Then we pick up where we were (until the next thing breaks).” That break-fix mentality seems to be in our DNA. Is there more we should be doing here? Is this holding us back in any way?

I’m not sure to what extent these problems or issues are tracked and categorized. I wonder if there is valuable information to be mined from these incidents that could enhance our reliability and resilience, and reduce the number of incidents or our response time to them. I now know how an HRO would answer that.

Over the years, I’ve become more and more aware of my personal blind spots and the blinders I wear based on my assumptions and past experiences. How do we as an organization become aware of our collective blind spots and the blinders we wear? What is our balance of specialist/generalist mindset? Practicing mindfulness may reveal some answers (and more importantly, equip us with the right questions to be asking).

**"Mindfulness"** – a rich awareness of discriminatory detail and an enhanced ability to discover and correct errors that could escalate into a crisis. (similar to situational awareness)

What I found to be even more eye-opening was a study on the lack of mindfulness, or **“mindlessness”**. Here are some quotes and comments that resonated with me (a few of them too much so):

- When people function mindlessly, they don't understand either themselves or their environments, but they do feel as though they do.
- Mindlessness is more likely when people are distracted, hurried, or overloaded.
- A tendency toward mindlessness is characterized by a style of mental functioning in which people follow recipes/runsheets, impose old categories to classify what they see, act with some rigidity, operate on automatic pilot, and mislabel unfamiliar new contexts as familiar old ones. A mindless mental style works to conceal problems that are worsening.
- Trouble starts when I fail to notice that I see only whatever confirms my categories and expectations but nothing else. The trouble deepens even further if I kid myself that seeing is believing. It's the other way around. Believing is seeing. You see what you expect to see. You see what you have labels to see. You see what you have the skill to manage.
- Surprises are inevitable. And with surprise comes the necessity to improvise, make do with the hand you are dealt, adapt, think on your feet, and contain and bounce back from unexpected events.

- To manage the unexpected is to be reliably mindful, not reliably mindless. Those who invest heavily in plans, standard operating procedures, protocols, recipes and routines tend to invest more heavily in mindlessness than in mindfulness.
- Traditionally organized companies are often their own worst enemy. They focus too much on their expectations, plans and past successes. This preoccupation impedes their ability to question their once-made expectations in order to gain a refreshed view of the current situation and properly respond to it.
- As a collective whole, we concentrate on what we expected to see happening, instead of paying attention to the many small and sometimes counterintuitive surprising observations that would have allowed different conclusions and decisions to arise.

Mindful practices help successful HROs find the right balance to the organizational dilemma that arises from the dual needs of a company to be open to change yet remain stable.

- They know that controlling and meticulously monitoring all predictable disturbances and problems is not enough. In addition, they work on countering their own tendency to rely on expectations of the future that are built on the past.

HROs develop stable mindful practices in order to recognize the things they never would have expected.

- This in turn enables them to change their routines and respond rapidly in a variable manner. Traditional organizations take the opposite route: Their perception is shaped by fixed routines and expectations. When confronted with conflicting perceptions, they are more likely to change their mindful practices than question their routines and expectations. For example, they prefer to modify their assessment criteria or ignore first signals to prove their expectations and routines.

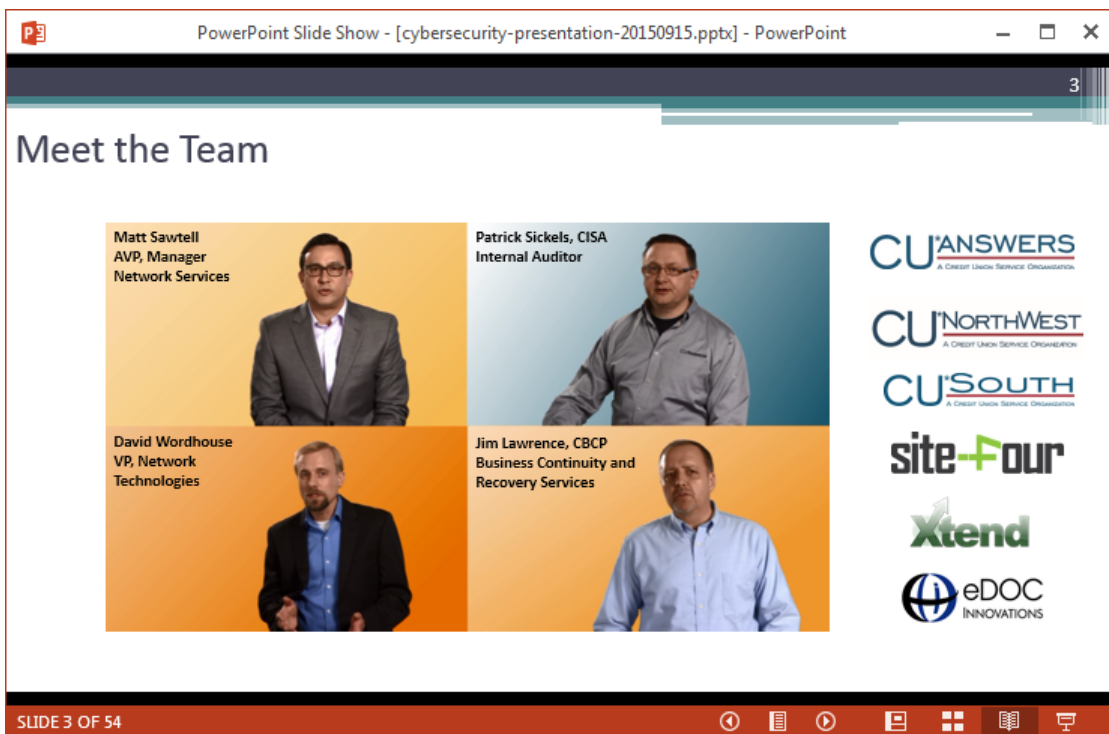
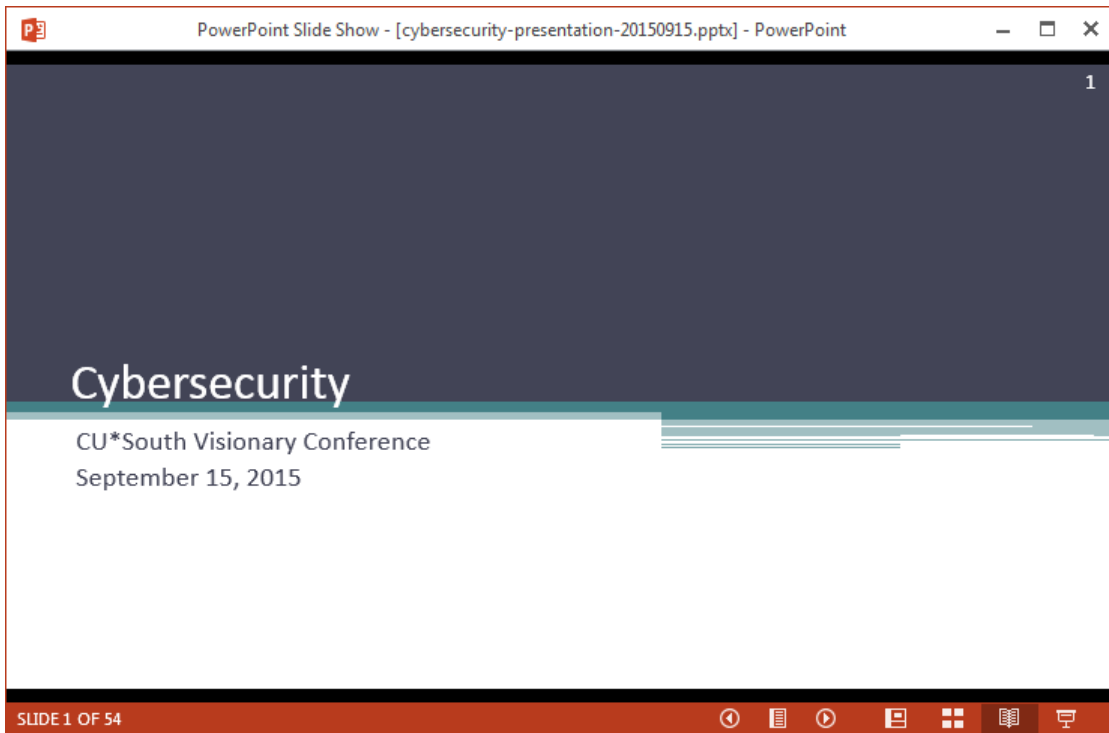
HROs are preoccupied with failure and surprises.

- Mistakes are not hastily viewed as an unwanted disturbance caused by human error, but are welcomed as a valuable source of information about the system. Mistakes reveal a great deal about how the entire system is functioning. How the problem evolved is of greater interest than who could be blamed. HROs devote time and energy to identifying all possible consequences of close calls (what do they teach us about the system?).

HROs are sensitive to operations

- A hierarchical mindset, which focusses attention from the bottom to top, combined with an obsession with plans and abstract numbers makes us blind to what is happening in the here and now. HRO's establish practices that encourage employees to improve their situational awareness.
- High reliability organizing differentiates itself from other organizing by its conviction that reliability does not occur through controlling stable conditions. Resilient performance results from making routines more flexible and, at the

same time, from developing and abiding from mindful practices that gradually influence company culture and management style.



PowerPoint Slide Show - [cybersecurity-presentation-20150915.pptx] - PowerPoint

4

## Network Resources (Brands)



- Cyber/IT Risk Assessment
- Strategic Technology Planning
- Security Policy Development
- Comprehensive Information Security Program (CISP)
- Business Continuity and Recovery Planning



- Firewall/Network/Systems Management and Monitoring
- Data Archive and Recovery
- Anti-Virus/Anti-Malware, Endpoint Protection
- Security Patching



- Concentration Risk Analysis
- BSA/ACH Reviews
- Daily Log Management
- CU\*BASE Security

SLIDE 4 OF 54

PowerPoint Slide Show - [cybersecurity-presentation-20150915.pptx] - PowerPoint

5

## Agenda and Goals

- Provide an overview of the cyber threats impacting the industry today.
- Define steps to assess and enhance cybersecurity preparedness at the credit union.
- Introduce tools and resources available to assist you.
- Invite you to connect after the presentation or after the conference.
- Resources used for the content of this presentation include:
  - NCUA
  - FFIEC
  - NIST
  - ISACA
  - PriceWaterhouseCoopers
  - Verizon Communications



SLIDE 5 OF 54



PowerPoint Slide Show - [cybersecurity-presentation-20150915.pptx] - PowerPoint

6

## The Connected World

**Internet of Everything**

Introduces new and unforeseen cyber risk dimensions.

**The Internet Of Everything**

Number Of Devices In Use Globally (In Thousands)

Source: BI Intelligence Estimates

SLIDE 6 OF 54

PowerPoint Slide Show - [cybersecurity-presentation-20150915.pptx] - PowerPoint

7

## State of Cybersecurity

“Despite millions of dollars spent on enhancements, cybersecurity remains the area of risk management with the **largest gap between threat and preparedness**.”

As the frequency and sophistication of cyber-attacks have increased significantly in recent years, counter measures have failed to keep pace. “

Financial institutions should seek to become **cyber resilient** by enhancing their risk management processes to better identify and monitor cyber threats.”

*A Closer Look - “Cyber: Think Risk, not IT” (April 2015, PwC)*

Common issues observed include:

1. Lack of enterprise-wide processes and governance
2. Insufficient security systems and controls
3. Reluctance to share information

SLIDE 7 OF 54

PowerPoint Slide Show - [cybersecurity-presentation-20150915.pptx] - PowerPoint

9


## Cybersecurity Defined

“The protection of information assets by addressing threats to information **processed, stored, and transported** by internetworked information systems.” [ISACA] *Information Systems Audit and Control Association*

“The body of technologies, processes and practices designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access.” [TechTarget]

Elements of cybersecurity include:

- Application Security
- Information Security
- Network Security
- Disaster Recovery/Business Continuity Planning
- End-user Education



SLIDE 9 OF 54

PowerPoint Slide Show - [cybersecurity-presentation-20150915.pptx] - PowerPoint

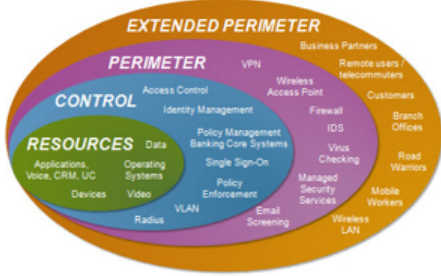
11

## Cyber Resilience

“The ability of a system or domain (network) to withstand cyber-attacks or failures, and in such events, to reestablish itself quickly.” [FFIEC]

**“Cyber Perimeter”**  
 An organization’s cyber vulnerabilities extend to all locations where its data is **stored, transmitted, and accessed** – by third party service providers, employees, and customers.

What used to be confined to data centers and connected terminals (ATM, wire transfer systems, etc.), now extends beyond the physical network to include cloud computing and mobile applications.



SLIDE 11 OF 54

PowerPoint Slide Show - [cybersecurity-presentation-20150915.pptx] - PowerPoint

14

## Current Threat Landscape

**Verizon 2015 Data Breach Investigation Report**

No industry is immune to security failures. Don't let a "That won't happen to me because I'm too \_\_\_\_\_" attitude catch you napping.

Cybersecurity is a risk management issue, not a technological one.

Top five industries affected (out of 20 identified in the study):

- Public
- Information
- Financial Services
- Manufacturing
- Retail



SLIDE 14 OF 54

PowerPoint Slide Show - [cybersecurity-presentation-20150915.pptx] - PowerPoint

30

## Cyber Risk vs. Investment/Effort

**Enterprise Approach Toward Cyber Risk Management**

		Organizational Risk Exposure	
		Lowest Risk	Highest Risk
Program Development	Highest Security	Higher Investment - Possible Inefficiencies	Optimal
	Lowest Acceptable Security	Optimal	Under Investment - Too Much Risk For Measures taken

Beyond Minimum Basic Regulatory Requirements and Agency Guidance - RM approach should scale to the credit unions level of risk exposure, appetite, complexity and perceived impact.

SLIDE 30 OF 54


PowerPoint Slide Show - [cybersecurity-presentation-20150915.pptx] - PowerPoint

31

## Regulatory Response (FFIEC)

### Cybersecurity Assessment Initiative (FFIEC)

- In 2014, the FFIEC piloted a cybersecurity examination work program at over 500 community financial institutions to evaluate their preparedness to mitigate cyber risks.
- On November 3, 2014, the FFIEC released a report titled “Cybersecurity Assessment General Observations” identifying the range of inherent risks and the varied risk management practices among financial institutions and suggesting questions for chief executive offices and board of directors to consider when assessing their institution’s preparedness.



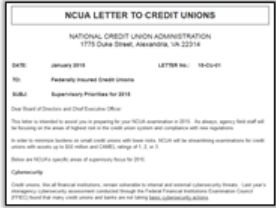
SLIDE 31 OF 54

PowerPoint Slide Show - [cybersecurity-presentation-20150915.pptx] - PowerPoint

32

## NCUA Letter 15-CU-01 - Cybersecurity

- Credit unions, like all financial institutions, remain vulnerable to internal and external cybersecurity threats. Last year’s cybersecurity assessment conducted through the FFIEC found that many credit unions and banks are not taking [basic cybersecurity actions](#).
- In 2015, NCUA will redouble efforts to ensure that the credit union system is prepared for a range of cybersecurity threats, focusing on proactive measures such as:
  - Encrypting sensitive data
  - Developing a Comprehensive Information Security Policy (CISP)
  - Performing due diligence over third-parties that handle credit union data
  - Monitoring cybersecurity risk exposure
  - Monitoring transactions, and
  - Testing security measures
- Field staff will also be evaluating credit unions’ capacity to recover and resume operations in the event a security breach does occur.



SLIDE 32 OF 54

PowerPoint Slide Show - [cybersecurity-presentation-20150915.pptx] - PowerPoint

45

## Cybersecurity Assessment Tool (FFIEC)

In light of the increasing volume and sophistication of cyber threats, the FFIEC has developed the Cybersecurity Assessment Tool to help financial institutions identify their risks and determine their cybersecurity preparedness. (Released on June 30, 2015)

### NCUA Implementation Timeline

**12-month Industry Implementation**

- National outreach efforts through 3/31/2016
- No formal exam or evaluation using CAT until 6/2016
- Select webinars to inform and provide training

**12-month Exam Implementation**

- Staff training
- CAT and exam aid development
- Field testing
- System development

**FFIEC Cybersecurity Assessment Tool**

**Overview for Chief Executive Officers and Boards of Directors**

In light of the increasing volume and sophistication of cyber threats, the Federal Financial Institutions Examination Council (FFIEC) developed the Cybersecurity Assessment Tool (CAT) to help financial institutions identify their risks and determine their cybersecurity preparedness. The Assessment provides a repeatable and accessible process for institutions to assess their cybersecurity preparedness over time. The Assessment incorporates cybersecurity-related practices from the FFIEC Information Technology (IT) Examination Handbook and regulatory guidance and coverage from other industry standards, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework.<sup>1</sup>

**Benefits to the Institution**

For institutions using the Assessment, management will be able to enhance their oversight and management of the institution's cybersecurity by doing the following:

- Identifying factors contributing to and decreasing the institution's overall cyber risk
- Assessing the institution's cybersecurity preparedness
- Evaluating whether the institution's cybersecurity preparedness is aligned with its risks
- Decreasing risk management practices and controls that are outdated or need enhancement and actions to be taken to achieve the desired state
- Refining risk management strategies

**CEO and Board of Directors**

The role of the chief executive officer (CEO), with management's support, may include the responsibilities to do the following:

- Develop a plan to conduct the Assessment
- Lead employee efforts during the Assessment to facilitate timely responses from across the institution
- Set the right tone of cybersecurity preparedness that best aligns to the board of directors' desired level of approved risk appetite
- Review, approve, and support plans to address risk management and control weaknesses
- Analyze and present results for executive oversight, including key indicators and the board, or an appropriate board committee

<sup>1</sup> The FFIEC updates the principles of the following: The Board of Directors of the Federal Reserve System, Federal Reserve Inspection Guidelines, Federal Open Market Administration, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, and State Liquor Control.

A complete version is available in [Appendix J, Strengthening the Resilience of Outsource Technology Services](#) in the [IT Examination Handbook](#).<sup>2</sup> For more information on the Assessment, visit [ffiec.gov](#).

June 2015

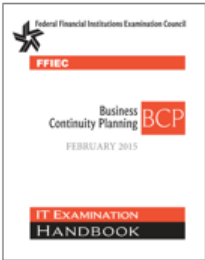
SLIDE 45 OF 54

PowerPoint Slide Show - [cybersecurity-presentation-20150915.pptx] - PowerPoint


42

## External Dependency Management

Domain #4



FFIEC  
Business Continuity Planning BCP  
FEBRUARY 2015  
IT EXAMINATION HANDBOOK



Appendix J: Strengthening the Resilience of Outsource Technology Services  
Background and Purpose

**FFIEC Business Continuity Planning Handbook - Appendix J: Emphasis on Four Key Elements**

- Third-Party Management
- Third-Party Capacity
- Testing with Third-Party TSPs
- Cyber Resilience

**Upcoming BCM Webinar**  
CU\*Answers University Class (60 min.)  
October 6, 2015 – 4:00-5:00 PM ET

**Business Resilience** : "The capacity to maintain functions and organizational structure in the face of an internal or external change or threat, recovery from a significant disruptions, and continue critical operations with minimal impact."

SLIDE 42 OF 54

PowerPoint Slide Show - [cybersecurity-presentation-20150915.pptx] - PowerPoint

53

## Review and Closing Remarks

- Review**
  - The Connected World (IoT)
  - State of Cybersecurity (Financial Services)
  - Cybersecurity Defined
  - Current Threat Landscape
    - Phishing
    - Common Vulnerabilities and Exploits (CVE)
    - Mobile Devices
    - Destructive Malware
    - POS/Payment Card Skimmers
    - Physical Theft/Loss
    - Human Errors
    - Risk Mitigation Controls
- NCUA/FFIEC Guidance (Regulatory Response)
  - Examiner's Top Ten
  - Cybersecurity Assessment Initiative/Tool
    - Gap between Inherent Risk and Preparedness Level
- Closing**
  - Remember: "Cybersecurity is a risk management issue, not a technological one."
  - See through the hype generated by opportunistic vendors.
  - Understand your organization and the environment it operates in (through the lens of cybersecurity).
  - Take advantage of resources available to you.

SLIDE 53 OF 54

### Final Comments:

With each step towards efficiency, automation and outsourcing, are we limiting our ability to detect (let alone manage) the unexpected? What does a balanced approach look like?

How can we detect when we've drifted off course and how do we correct our sails? Who's up on the mast looking out over the waves?

How are we contributing to the blind spots of the credit unions we serve (assumptions, expectations, etc.)?

One of my favorite TV shows is called "Brain Games" (National Geographic channel) <http://braingames.nationalgeographic.com/>. I have several episodes recorded on my DVR. With each one I watch, I'm finding myself trusting how my brain interprets the information received through my senses less and less, especially my eyes. It's also fascinating how two (or more) people can see/experience the exact same thing and interpret it very differently.

**Jim Lawrence** | CU\*Answers | Manager, Business Continuity and Recovery Services | CBCP

[jim.lawrence@cuanswers.com](mailto:jim.lawrence@cuanswers.com)

## A Compliance Perspective

*Jim Vilker, NCCO, CAMS, CU\*Answers VP Professional Services*

This is a very interesting article. What I found interesting is how the author described a typical organization “We implicitly subscribe to a theory of the organization as a highly monolithic, predictable entity, - one in which members can be easily programmed to plod along monotonously, facing the same kinds of problems day after day and year after year”. He further goes on to say “When the unpredictable does happen, and the world as we know it unravels, we are all the more likely to become so paralyzed that we cannot survive the experience.”

In my opinion and on a spectrum of complicit to HRO we are much more an HRO than most organizations or credit unions we serve. Why? We must be as we are the financial ledger for millions of Americans and the core system our cooperatives run on.

Now I am not saying that we must be thinking of failure on a constant basis as described in the nuclear power plant analogy as that would stymie any and all creativity and innovation. However, our level of mindfulness is inherent and is culturally part of our organization. As a matter of fact most if not all senior managers in this organization kick the hell out of themselves when we miss the small things that have across the board large implications (mindfulness). We are trained to watch for the burning embers that could potentially cause a forest fire.

Another example are the times this organization puts everyone on notice that something has happened and we all must step up to the plate? An example would be when we have to call a “data integrity issue” relative to the software. Another would be our culture of resilience as practiced by our HA rollovers (no other data processor practices like we do). Another example is our CEO incident reports. As part of our culture we are trained that nothing is to be held so close that others are not aware of an impending issue, failure, or potentially disastrous event.

Because of that fact senior staff understands what is happening in the weeds and if we do not communicate we will not have careers at CU\*A for very long.

The “cosmology” as it relates to responding to critical events or circumstance is also an interesting topic. What I take away from this section is how organizations react when something absolutely does not make sense and they tend to think in a reflective manner as they always have. I am not sure how to assimilate that in our organization. We, by nature, must think out of the box by virtue of our product structure and the ever changing environment and in many cases in a reflective way but one that must morph at the drop of hat. We do respond to many diverse situations but the way it is explained in this article is that what was black is now white and during critical events make decisions based upon new universal principals.

Finally from a regulatory perspective and as the article refers to HROs typically live in a state of chaos. My contention is that our regulatory bodies have created a state of chaos which we have never seen before in our industry. This in affect has also moved us more to the side of an HRO. We never know what is coming next, continuously have to monitor the pulse, and be prepared to react quickly and with urgency when the CFPB makes a regulatory change. An example of that would be the mortgage statement requirements brought on by Regulation Z. The regulation was published giving service providers over a year to complete the programming yet subsequent interpretations continued on through August with a January deadline. We had to code for this change in less than three months on a project that actually should have taken almost a year. Chaos? That is the definition of what is happening in regulatory circles and forcing us to be more mindful.

There are numerous examples in this organization and history that would indicate we bend more towards being an HRO than most classic organizations. The question of how we test the perception maybe should be more how do we verbalize internally and externally those things we do every day relating to our reaction to critical issues.

**Jim Vilker** | NCCO, CAMS | CU\*Answers VP Professional Services

[jvilker@cuanswers.com](mailto:jvilker@cuanswers.com)



## An Auditor's Perspective

*Patrick Sickels, CU\*Answers Internal Auditor*

The central thesis of *Sense and Reliability* is that Highly Reliable Organizations (“HROs”) have fewer accidents than the norm despite greater risks, due to a culture of mindfulness that embrace complexity and are therefore more sensitive to weak signals that portend danger. The question presented is whether the principles of mindfulness and HROs can be applied to cybersecurity as part of a business strategy to deliver more services via the Internet and other public network infrastructures. The answer is yes, but with some qualms.

As background, [HRO philosophy comes from and as part of Normal Accident Theory](#). Normal Accident Theory or (“NAT”) argues that accidents are inevitable in complex systems because, among other reasons, the systems are too complex to accurately predict their interoperability in all environments. [The ‘normal’ part simply means that the system is acting in an expected way that cannot be foreseen because of some other event, such as operator error.] From the cybersecurity aspect, this theory is clearly fundamentally correct. It is not possible to fully predict how [an update might create a security vulnerability where none existed before](#), or [where one technological behemoth might let the world know a vulnerability exists before a patch is ready](#). A system’s susceptibility is usually defined by two important elements.

One is *interactive complexity*, which means that there are so many outcomes that are not immediately visible when the environment changes it isn’t possible to track all of them. Another is *tight coupling*, meaning the system is highly interdependent. A change to one element to the system affects them all. In the cybersecurity realm, an example of this would be where a change in software allows more data to be accessed than should be allowed. An example of this would be [Heartbleed](#). Heartbleed by itself may not be a critical vulnerability; what matters is what system is vulnerable, whether this system can be used for future attacks, and what kind of data can be retrieved. Another example is the [Target Breach](#). It is highly unlikely that the retail giant could have ever thought or suspected a cybersecurity breach at their HVAC vendor could culminate in a successful attack on their point of sale systems.

A flaw with NAT is that it is overly pessimistic. NAT suggests that we should be having plane crashes, power plant explosions, and other disasters at a rate much higher than we actually do. In opposition to this, HRO is far sunnier, and argues that [if you provide the people in organization with mindful attention to the complexities faced](#), the less likely accidents will occur. HRO philosophy is that management that embraces complexity will be far more capable of managing unexpected events, including severe ones such as “cosmology episodes” or black swan events. In effect, the human system compensates for technological error. Of course, HRO theory is fundamentally correct as well. Organizations that react well to small signals of trouble often can stop small issues from escalating into larger ones. [WalMart has been praised for its effectiveness in responding to disasters](#); far better than the U.S. government has in fact.

However, there is some reasonable criticism of HRO theory as well. The number of critical failures in areas such as aircraft carriers is [much higher](#) than HRO theorists estimate. (There's probably been nearly [10,000 deaths](#) around aircraft carriers since 1948). There are also probably far more significant errors at nuclear power plants than HROs estimate; it's just that there are only three that were potentially or actually so catastrophic that they are by-words for the industry – Three Mile Island, Chernobyl, and Fukushima.

In addition, HRO theory rather blithely assumes that organizations have the resources to do massive investigations to ensure painstaking investigations. An example used is that of a nuclear power plant that shuts down the plants air supply system in response to an emergency signal. The plant operators won't just rely on the blueprints, but instead will "check the whole system for valves, piping, or reroutes that may have been added since the drawings were completed." Certainly, this might be encouraged or even necessary for a nuclear power plant, but is that really possible in the business world we could shut down our software for days for testing if a vulnerability is found? At some point, you patch the vulnerability and you have to keep going. How would you even test across the organization to ensure every possible permutation of risk facts has been met?

There is also the signal to noise ratio problem, which is poorly addressed by HRO theory. The Target Breach remains a good example of this. Target IT staff [actually detected the breach when it occurred](#); they didn't take action because it looked just like the same alerts the staff received hundreds of times on a daily basis. Per the article:

*The alert from [the security vendor] labeled the threat with the generic name "malware.binary," according to Bloomberg Businessweek. Two security experts who advise organizations in responding to cyber attacks and both have experience using [the] technology said that security personnel typically don't get excited about such generic alerts because [the security vendor] does not provide much information about those threats.*

***The experts said that they believed it was likely that Target's security team received hundreds of such alerts on a daily basis, which would have made it tough to have singled out that threat as being particularly malicious.***

*"They are bombarded with alerts. They get so many that they just don't respond to everything," said Shane Shook, an executive with Cylance Inc. "It is completely understandable how this happened." [emphasis added]*

Almost certainly, if Target had made it so these alerts were not so frequent, the attack would not have been detected at all. HRO theory argues that a mindful organization will investigate these thoroughly and embrace the complexity it represents. The reality is that from a business standpoint such embracing is not usually practical for even huge organizations; certainly not possible with smaller scale companies.

However, this does not mean CU\*Answers shrinks from the challenges of mindful thinking. CU\*Answers attacks the challenge of complexity and risk mitigation by following core risk management rules:

- Admitting error, both human and system
- Ensuring we have ‘Lessons Learned’ when we revisit accidents or problems
- Accountability is baked into team and job responsibilities
- Reviewing routines and suggesting improvements
- Documentation is a way of life
- “I don’t know but I will find out” is an acceptable answer
- Redundancy is built on critical systems
- Evaluation of what is critical is made regularly
- Protocols are created to provide teams with a framework to follow, but teams are also given freedom to think through and bring solutions to management in a crisis
- Contrary opinions are encouraged
- Testing is extensive
- Accepted risks are documented
- Contracts limit liability
- Insurance coverage is there as a backdrop
- Our company is a cooperative, and everyone has a stake in the organization’s success, especially client/owners

No organization is perfect, but there is a balance here by embracing mindfulness and HRO concepts with the needs of the business.

**Patrick Sickels** | CU\*Answers | Internal Auditor

[psickels@cuanswers.com](mailto:psickels@cuanswers.com)

## Balance and Motion are the Key

*Dave Wordhouse, VP Network Technologies, CU\*Answers Network Services*

Interesting article.

Weick doesn't seem to make a distinction between applying his principles to tactical or strategic applications and implies they are suitable for either.

There seems to be some logical inconsistency concerning his remarks about planning in regards to the operation of aircraft carriers and nuclear power plants that don't seem to translate to the construction of those highly complicated machines. I can say that our success rate for implementing complicated infrastructure like networks improves dramatically the more granular the planning is – the more we try to anticipate what will go wrong (which the article says we shouldn't spend time doing) the smoother the project tends to execute. The perspective seems to work better from an operational standpoint, which is consistent with the examples provided.

At any rate, the ability to detect, adapt, compensate and adjust to changing conditions is certainly important. Weick's comments about looking while leaping remind me of advice from one of my kayak instructors: if you start to flip, take a stroke – any stroke. Taking instant action by getting a blade in the water provides immediate stability regardless of whether or not it provides forward motion. A kayak with the smooth side down is always faster than when the skipper is swimming. Stay upright, correct, and GO. I think there are parallels to this theory here.

Here are the HRO attributes/principles I noticed in the article. Did you see these, or something else? Where do we align and where don't we and where do you agree?

- HRO leaders do not try to predict what will happen next or how people will react
- HRO leaders realize decisions they make may have unintended consequences
- HRO leaders will take action at the earliest sign of danger
- HRO leaders are constantly concerned with failure
- HRO leaders are focused on the front line employees “where the real work gets done” as those people have the real expertise
- HRO leaders do not oversimplify problems or reality – they do deep dives and act
- HROs need a broad team with diverse skill sets complimenting each other, to best deal with the unexpected
- HROs believe understaffing, poor handoffs between teams, and low frequencies of performing a task are real causes of failure
- HROs don't punish failure, they learn from it
- HROs don't take shortcuts
- HROs value generalists over specialists

- HROs avoid analysis-paralysis
- HROs take action, sometimes in the middle of studying the issue
- HROs know that plans are “just signals, games, and excuses for interactions.” They can’t be fully trusted and are subject to change at any time, shouldn’t be fully relied upon, and can deceive into thinking you know more than you do
- HROs practice executing against the unexpected

In follow-on research, these are also traits of HROs:

- Highly trained personnel
- Continuous training
- Effective reward systems
- Frequent process audits
- Continuous improvement efforts

As with anything, balance is important. Acting immediately at the first sign of danger could be perceived as alarmist so the response might need to be carefully crafted. In reality, it’s not alarmist but a signal for adjustment, which parallels our internal process of X went wrong so we implemented Y to prevent a recurrence. This is tactical minded thinking that places high values on feedback loops to help sense impending issues. These adjustments dovetail with sustainability as threats to revenues should be acted upon as part of that feedback loop, just as one might to any other risk factor. Balance and motion seem key to the theory.

**Dave Wordhouse** | CU\*Answers Network Services | VP Network Technologies

[dwordhouse@cuanswers.com](mailto:dwordhouse@cuanswers.com)

## Rational Business Decisions, not Emotional Responses

*Matt Sawtell, VP Network Technologies, CU\*Answers Network Services*

This was a good article and has led me down the path of some additional reading over the past few days. I will admit it was my first exposure to this particular work and it's interesting to see the many similarities between HRO as an organizational discipline and many of the processes that have grown logically, though organically at CU\*A. Also interesting is the growing attention on this in the financial and medical industries as we all look for ways to further reduce risk within our organizations. Though the specific controls for an FI mitigating cyber threat is much different than those controls used by Navy to prevent accidents on an aircraft carrier, the concepts certainly apply to both.

The two leading thinkers on this subject, and from whose studies much of the information in the HBR article was pulled (Weick and Sutcliffe) were specific to break down Mindfulness for an HRO into 2 categories: Anticipation and Containment. In each category are some thoughts and observations on how we at CU\*A have put some of the concepts into practice (many from my CNS centric point of view).

### Anticipation

Preoccupation with failure:

**We have best practices** - Within the company, we have a number of evolving sets of best practices, from our employee security manuals, specifically on the CNS Team our handbook, etc. We train on these practices and encourage team members to push improvement into the process from all levels.

**We recognize failure as an opportunity** – The process for moving forward from a crisis, critical event or near-miss is important. We commemorate these instances as opportunities to review and improve processes – a robust gap analysis happened during heartbleed and the other 0 day vulnerabilities of last year and with each subsequent event, our processes improved. We do the same for all HA and BC testing, both on the core and for credit union clients.

Reluctance to simplify:

This is a key within the CNS processes when dealing with negative outcomes from both regular processes and from unplanned events. IT and cybersecurity offer many opportunities to say “the problem seems to have cleared up, we are good to go”. We realize that we need to also say “we’ve identified the root cause of the issue and know it won’t happen again”. Without that focus, and frequent reexamination of an issue, we put ourselves at risk of having cured the symptoms but not the actual issue, resulting in future instability, loss, etc.

Sensitivity to operations:

For both internal (CUA and CUSO partners) and external (client CUs) we have an operations team that runs through various critical tasks on a regularly prescribed basis. This team works from robust documentation that helps us identify instances where systems or networks are not operating in a normal range. We encourage these team members to “sound the alarm” at the first sign of danger, as it’s much easier to resolve a small issue before it turns into a large one. A key component of our approach here is also to require transparency, meaning that if an incident is detected, and the response isn’t acceptable at the first level, the front line operations team is encouraged to run their concern directly to the executive level, and correspondingly, management is regularly in touch with and closely communicating with this team.

I would attribute the execution of these teams to much of our ability to proactively respond to the situations that, as we know are not a matter of “if” but “when”.

## **Containment**

Commitment to resilience:

CU\*Answers has developed a robust plan for business continuity, across a number of fronts and with consideration to standard risk management principles. We test the controls regularly to ensure they function. We perform gap analysis to drive improvement into the process.

In addition to the set of technical capabilities, I see this as something approached in non-technical ways across the organization and in this capacity see it better stated as a commitment to relentlessness.

CU\*Answers as an organization has a continuous drive to improve processes in all facets of business, from a focus on formal training and education to a management hierarchy that puts emphasis on not just what to do but why. While many of the characteristics would strengthen an HRO, this one obviously equates to the success of the enterprise in general.

Deference to expertise:

In any high risk situation, we want to be able to draw on expertise, as opposed to authority. One of the things we tell new team members when they start is, google is great, but really successful team members don’t know all the answers, they know who the experts are. In IT this is key – with subject matter so broad, no one person, no matter how senior their position is an expert in everything. We encourage expertise on the team as leaders, opposite the above point, by making a point to, during conversations, ask why or why do you do it this way. We also align team goals at all levels with “how would you improve the process” – valuable feedback comes from all levels within the organization.

Overall I think we are doing a good job here, but as we know and these concepts note, there is always room for improvement. I do believe there to be value in carrying this conversation forward to the CU world, both in terms how and why CU’s can be

effective HROs and how we can contribute, both as practitioners and as a provider of tools and tactics. I believe that just starting to think like an HRO can improve the quality of an organization's posture without the necessity of fancy tools and services.

As to your final point, with concern to fear mongering, balance is key - cyber risk needs to be managed; it can't be eliminated. Once you realize you can't eliminate it, everything else can be classified, prioritized and dealt with as a rational business decision and not the emotional response to someone yelling fire in the theatre.

I believe this will be a constant focus that we will address thoughtfully for each threat. As a provider of many cybersecurity services I constantly hear, "why don't you offer this" or "why do I need to buy this too?" We need to be very clear to the market on both what (and why) we do this AND why we don't do the other things.

Thanks for the opportunity to do some exploration on this – look forward to future conversations

**Matt Sawtell** | CU\*Answers Network Services | AVP Managed Technology Services

[msawtell@cuanswers.com](mailto:msawtell@cuanswers.com).



ORGANIZATIONAL CULTURE

# Sense and Reliability

by Diane Coutu

FROM THE APRIL 2003 ISSUE

## The Idea in Brief

Stable. Secure. Predictable. Many of us describe our organizations in these reassuring terms. But companies face numerous *un*predictable challenges that strain our imaginations and creativity. A complacent view spells danger: When the unpredictable *does* happen, we become too paralyzed to survive the experience.

How to better manage the unpredictable? Take lessons from high reliability organizations. HROs—nuclear power plants, hospital emergency rooms, firefighting units—constantly operate under trying conditions. Yet they have surprisingly few accidents. Why? **Mindfulness**: the power to detect—and act on—even weak signals of impending danger.

Most of us spend our lives operating in some kind of organization—whether it’s a family, a church or synagogue, a school, or a company. And, as we do with many of our close relationships, we take a lot for granted about these groups. Indeed, our familiarity with them often breeds a kind of contempt: We blame organizations for subjecting us to deadening routines and demanding from us dehumanizing conformity. We implicitly subscribe to a theory of the organization as a highly monolithic, predictable entity—one in which members can be easily programmed to plod along monotonously, facing the same kinds of problems day after day and year after year.

But that view is deeply flawed; most organizations face all kinds of unpredictable challenges—large and small—that collectively place huge demands on people’s creativity and imaginations. Indeed, in an ever-changing, rough-and-tumble business environment, the assumption that the corporation is something stable and secure becomes dangerous. When the unpredictable does happen, and the world as we know it unravels, we are all the more likely to become so paralyzed that we cannot survive the experience.

What can we do to better recognize and manage the unpredictable? Few people are more qualified to answer that question than Karl E. Weick, the Rensis Likert Distinguished University Professor of Organizational Behavior and Psychology at the University of Michigan Business School at Ann Arbor, and professor of psychology at the university. Over the course of his career, Weick has become world renowned for his insights into why people in organizations act the way they do. His book *The Social Psychology of Organizing* (McGraw-Hill), first published in 1969, turned organizational psychology on its head by praising the advantages of chaos, demonstrating the pitfalls of planning, and celebrating the rewards of “sensemaking.” These insights were expanded in a later book, *Sensemaking in Organizations* (Sage, 1995). Most recently, Weick—along with University of Michigan colleague Kathleen M. Sutcliffe—has turned his attention to *Managing the Unexpected* (Jossey-Bass, 2001).

Weick has journeyed widely in his search for organizational meaning—from jazz orchestras to firefighters, from the Skylab crew to Native American hunting parties—and his findings stand in sharp contrast to most of the literature on business organizations. Weick’s view of corporations is as complex as the people who populate them. His organizations chat, dissemble, disguise, mobilize, and “galumph.” In other words, they are alive. Not surprisingly, while most management writers advise businesspeople to simplify and streamline, Weick challenges executives to complicate themselves. For him, reality is not some black-and-white matter “out there,” but rather a fluid entity that organizations half imagine and half create. In the following edited conversation, Weick offers fresh perspectives on managing surprise, focusing on failure, and surviving what he calls “cosmology” attacks.

Your most recent research focuses on high-reliability organizations. What are HROs, and why are they important?

An HRO is, for instance, a nuclear power plant, an aircraft carrier, an air-traffic-control team, a fire fighting unit, or a hospital’s emergency department. You could even think of restaurant kitchens, with orders coming in rapid-fire and knives flying all over the place, as high-reliability organizations. HROs operate under very trying conditions all the time and still manage to have fewer than their fair share of accidents. An aircraft carrier, for example, could have a disaster every time a plane lands or takes off. But it doesn’t, and the question is, Why not?

The key difference between HROs and other organizations is the sensitivity or *mindfulness* with which people in most HROs react to even very weak signs that some kind of change or danger is approaching. In contrast to HROs, most companies today are hugely unprepared for the unpredictable. Managers are under the illusion that they know more or less what’s going to happen next or how other people are likely to act. That’s both arrogant and dangerous. Not only do those managers ignore the possibility that something unexpected will happen but they also forget that the decisions they do make can have unintended consequences. Consider the launch of New Coke in 1985. Immediately after the product was introduced, the company got as many as 8,000 letters a day from angry consumers. Clearly, Coca-Cola had failed to accurately predict people’s behavior. To its credit, however, the company came back with Coke Classic within just three months. But as the story shows, you have to take action at the earliest sign of danger, or you may get killed. Everyday problems escalate to disaster status very quickly when people don’t respond appropriately to signs of trouble. HROs distinguish themselves by being able to detect incredibly weak warning signs and then taking strong, decisive action.

How might an HRO respond to a weak signal?

Consider board operators in the control room of a nuclear power plant. They pay close attention to small, unexpected events that may foreshadow larger system problems—for instance, they note when an automatic system doesn’t respond as expected or when unusual data regarding plant parameters crops up. They recognize when a procedure is inappropriate and navigate to a different one. This watchful updating facilitates management of the unexpected, and I believe it results in large part from a preoccupation with failure. Think about it: Concerns about failure are what give nuclear power plants their distinctive quality. But since complete failures in nuclear power plants are extremely rare, the people working there are preoccupied with something they seldom see. And this requires a special kind of alertness. Workers in these facilities do not monotonously watch dials, read printouts, or manipulate graphic displays and then breathe wearily at the end of the day: “Terrific—I’ve just had another dull, normal day.” On the contrary, these workers make judgments and adjustments and comparisons to *keep* their days dull and normal. Of course, there is undoubtedly a kind of obsessiveness in all this, which is true of all HROs and which can make them unpleasant places to work in. But the minute a nuclear-plant worker says, “Hey, this job is boring,” there is the danger that he’ll stop making the fine-tuned adjustments needed to keep the job unexciting. And we all know how catastrophic it can be when things get exciting in a nuclear power plant.

For a classic example of a company misreading or ignoring a weak signal, you might consider the staffers at Ford's recall office during the Pinto crisis in the 1970s. They were aware that the Pinto could sometimes catch fire in low-speed, rear-end collisions. But they saw no need to recall the car, because they couldn't find a "traceable cause" for the incidents. They missed the fact that bolts on the cars' rear axles had punctured the gas tanks of the Pintos involved in those crashes. Their inability to pick up on weak signals spelled disaster.

Can organizations learn to be more mindful?

They can, by adopting some of the practices that high-reliability organizations use. For instance, besides being fixated on failure, HROs are also fiercely committed to resilience and sensitive to operations. Managers at these organizations keep their attention focused on the front line, where the work really gets done. For example, among wildland firefighters, the most successful incident commanders are those who listen best to the people out there actually fighting the fires. HROs also defer to expertise, and they refuse to simplify reality. This last point is particularly important because it has profound implications for executives. As I have often written, leaders must complicate themselves in order to keep their organizations in touch with the realities of the business world. My worry when executives say, "Keep it simple, stupid," is that they're underestimating the complexity of their own organizations and environments. But contrary to how we often think about them, organizations are not at all passive; they are extremely active, and they half create their environments. So part of the solution to managing the unanticipated is to get executives to step back and acknowledge just how messy reality can sometimes be.

**My worry when executives say, "Keep it simple, stupid," is that they're underestimating the complexity of their own organizations and environments.**

That reminds me of your famous battle cry: "Believing is seeing."

Simple as it sounds, I really do think that's the case more often than not. By inverting the cliché, I'm trying to communicate that we can only see what we are prepared to see. There are many illustrations of this fact, but the one that really drove it home for me was the story of how child abuse first came to be recognized in this country. Child abuse was "discovered" and the treatment of it accelerated only in the 1960s when, in Boulder, Colorado, pediatricians and radiologists who were treating children added social workers to their teams. Until then, the pediatricians and radiologists wouldn't even allow the possibility that parents could be hurting their own kids because they didn't know what to do next. But when the social workers came on board, they said, "Sure, child abuse happens, and we know how to handle it by providing protective services." It was only at this point that the physician teams could afford to see child abuse, because then they knew how to deal with it. The moral, of course, is that the greater the repertoire of responses you have on your team, the more things you can do. And ultimately, the more ready you are to deal with reality, the more you can acknowledge its complexity. That's one of the reasons, I think, that we are seeing more concern about greed and CEO conduct in the United States right now—because we now feel we have a better idea what to do about it through governance.

You say HROs are obsessed with failure. But don't most organizations marginalize leaders who fail?

There is a strong tendency in companies that aren't high-reliability organizations to isolate failure, to blame the culprit, and to not learn from mistakes. And that's idiotic, because few failures can be traced to a single individual. Consider excess surgical deaths in hospitals. Typically they are the consequences of understaffing, poor handoffs of information about the patient as he is moved from the surgical suite to the recovery room and then to the ward, and the low frequency of performing a particular operation. But no matter how many people may be involved in them, failures are easier to recover from if they are spotted early on, when they are small. If you can catch a failure right away, it's less difficult to say, "Look, there's been some kind of mistake here, but it might just be a sign that the system has gone a little haywire."

Organizations can do a lot to encourage their members to face up to failure, even to become preoccupied with it. There is an interesting story that one of my colleagues tells about the great German scientist Wernher von Braun. When a Redstone missile went out of control during prelaunch testing, von Braun sent a bottle of champagne to an engineer who confessed that he might have inadvertently short-circuited the missile. An investigation revealed that the engineer was right, which meant that expensive redesigns could be avoided. You don't get a lot of admissions like that in organizations today. But all it takes is one such story to make an individual in the company buck up and say, "Hey, these folks are serious about facing up to failures, so I'm going to take a chance and speak up."

I've also repeatedly found that employees at HROs cultivate a fascination with failure by refusing to take shortcuts or simplify reality. Let's say the workers at a nuclear power plant have to shut down the plant's air supply system in response to some emergency signal. They won't treat the plant blueprints as a reliable guide for the system—which a businessperson might do in the interest of getting the job done quickly. Instead, they will check the whole system for valves, piping, or reroutes that may have been added since the drawings were completed. They know that it's what's missing from the blueprints that could cause the really serious surprises. In other industries as well, successful companies often turn out to be those that refuse to simplify reality—that go behind the blueprints. I'm thinking of companies like retail giant Wal-Mart, with its legendary attention to detail; the California-based design group Ideo; and Francis Ford Coppola's American Zoetrope Productions.

Is there one kind of leader who's particularly good at managing the unexpected?

Not surprisingly, newcomers to an organization catch a lot of stuff that old-timers miss, which is one reason there is such a huge temptation to bring outsiders into an organization during crises. But newcomers, for good reason, also tend to shut up about what they see, lest they come across as really dumb. That's why I place a lot of trust in executives who are generalists. People who study liberal arts tend to get exposed to a wider variety and greater richness of values than people normally get in professional schools. At the same time, though, when I speak of generalists, I mean more than those people who have studied literature or art in college. I'm talking mainly about executives who have heterogeneous work and industry experiences. Because of their diverse work histories, these executives are in a good position to cope with problems in original ways. I'm thinking here of Lou Gerstner, who landed at IBM with the experiences he had gained at RJR Nabisco, a consumer products company; American Express, a financial services company; and McKinsey, a consultancy. Also consider the late Mike Walsh, who moved from Cummins Engine to Union Pacific Railroad and Tenneco, and Larry Bossidy, who joined Allied Signal from General Electric. Generalists such as these can often construct a richer, more useful version of what's going on than specialists can. At the very least, their broad experiences can help these executives not to get paralyzed by what I call a "cosmology episode."

That's an intriguing term. Can you explain it?

Think back to 1993. That's when the Centers for Disease Control first came up against hantavirus in the Southwest. The virus made no sense: It had never appeared in landlocked regions before, and it was killing people by attacking their lungs rather than their kidneys, the virus's usual target. It seemed to defy explanation. And that's as close a parallel to a cosmology event as I can describe. Basically, a cosmology episode happens when

people suddenly feel that the universe is no longer a rational, orderly system. What makes such an episode so shattering is that people suffer from the event and, at the same time, lose the means to recover from it. In this sense, a cosmology episode is the opposite of a déjà vu experience. In moments of déjà vu, everything suddenly feels familiar, recognizable. By contrast, in a cosmology episode, everything seems strange. A person feels like he has never been here before, has no idea of where he is, and has no idea who can help him. An inevitable state of panic ensues, and the individual becomes more and more anxious until he finds it almost impossible to make sense of what is happening to him.

The continual merging and divesting and recombining and changing of responsibilities and bosses over the years has created intense cosmological episodes for many businesspeople. Even senior executives are unsure of whom they're working for and why. If you compound that with more globalization and high-velocity change in the environment, it's not surprising that nobody seems to have a firm sense of who they really are any more. Many people even have trouble locating themselves on organizational charts. So I think it's fair to say that in the course of their careers, most managers will have at least one cosmology episode; their worlds will get turned upside down. Having the kind of alertness to weak signals that we see at HROs can help managers avoid this particular psychological crisis. In the case of the hantavirus, for example, the puzzle was eventually solved when epidemiologists discovered that recent climatic changes had produced an explosion in the rodent population that carried the virus, which increased the likelihood that humans might be exposed to hantavirus. In cosmological episodes, paying very close attention to details can definitely restore a sense of mastery.

## A cosmology episode happens when people suddenly feel that the universe is no longer a rational, orderly system.

So people can convert a cosmology episode into something positive?

What I've repeatedly noticed is that the people who really get in trouble during these crises are those who try to think everything through before taking any action. The problem with defining and refining your hypotheses without testing them is that the world keeps changing, and your analyses get further and further behind. So you've got to constantly update your thinking while you're sitting there and reflecting. And that's why I'm such a proponent of what I call "sensemaking." There are many definitions of sensemaking; for me it is the transformation of raw experience into intelligible world views. It's a bit like what mapmakers do when they try to make sense of an unfamiliar place by capturing it on paper. But the crucial point in cartography is that there is no one best map of a particular terrain. Similarly, sensemaking lends itself to multiple, conflicting interpretations, all of which are plausible. If an organization finds itself unsure of where it's going, or even where it's been, then it ought to be wide open to a lot of different interpretations, all of which can lead to possible action. The action and its consequence then begin to edit the list of interpretations down to a more manageable size.

And this is the point I wish to underscore: Action, tempered by reflection, is the critical component in recovering from cosmology episodes. Once you start to act, you can flesh out your interpretations and rework them. But it's the action itself that gets you moving again. That's why I advise leaders to leap in order to look, or to leap while looking. There's a beautiful example of this: Several years ago, a platoon of Hungarian soldiers got lost in the Alps. One of the soldiers found a map in his pocket, and the troops used it to get out safely. Subsequently, however, the soldiers discovered that the map they had used was, in fact, a drawing of another mountain range, the Pyrenees. I just love that story, because it illustrates that when you're confused, almost any old strategic plan can help you discover what's going on and what should be done next. In crises especially, leaders have to act in order to think—and not the other way around.

One of the cruelest things about organizations today is that they hold executives to standards of rationality, clarity, and foresight that are unobtainable. Most leaders can't meet such standards because they're only human, facing a huge amount of unpredictability and all the fallible analyses that we have in this world. Unfortunately, the result is that many executives feel they just can't measure up. That triggers a vicious psychological circle: Managers have rotten experiences because they keep coming up short, which reinforces low self-esteem. In the end, they get completely demoralized and don't contribute what they actually could—and otherwise would.

But if you tried telling today's leaders to accept the fact that they're not quite as rational, deliberate, and intentional as they claim to be—and that that's okay, because that's the way humans are—I think most executives wouldn't understand. They've internalized the pressure to be perfect. Caught in a nasty cycle of insecurity that is covered up by hubris, many executives place a lot of hope in unrealistic goals. Meanwhile, it is the people further down in the organization who are actually doing all the improvising and patching and scrambling to make plans work. And the people at the top don't have any idea how much the people in the middle are breaking their backs to keep the organization going.

What does sensemaking have to do with our instinct to create stories to explain the unexpected?

As the writer Joan Didion once put it, "We tell ourselves stories in order to live." In business, we tell ourselves stories in order to know more and compete better. In a crisis, stories help us not to panic. As reality unfolds, everyone starts asking themselves, "Do you have any idea what's going on here?" Then someone spins a story, and the moral is something like, "Don't worry, I have seen something vaguely like this before." And that's more than comforting, it's motivating. People don't need much to get moving—just a little kernel of meaning. Even if the company is in a quite serious situation, someone will be able to use that tiny core of meaning to convert their interpretations into action.

In any organization, the most powerful stories are created and spread through informal gossip. Indeed, I don't think there's a fundamental difference between gossiping and storytelling. Gossiping is just a way to rehearse different stories before they become formalized and spread out across the organization. It can help employees process information that might not otherwise make it into the "official" story. At the same time, because it is mostly made up of exaggerations and bluster, gossip can help prepare an organization for the unexpected and, in this way, can serve as a prelude to sensemaking and action. Indeed, I'm always surprised by how little factual information leaders really need to get going.

Let me give you an example. One organization that has struggled with reliability is Union Pacific. Back in the 1990s, the company suffered repeatedly from managerial paralysis—even the employees began to call it the Utterly Pathetic railroad. At that time, the following story started circulating among employees and customers: A locomotive engineer got so fed up with the railroad's incompetence that he decided to commit suicide. So he went outside, lay down on the railroad tracks—and starved to death. That kind of urban myth was a perfect way to express just how frustrated people had become with the railroad not doing anything during a period of intense upheaval.

You've often said that plans are overrated, that they can actually make things worse for organizations.

Yes, I usually urge executives to fight their tendency to want to plan everything. Most plans are too specific, and the details create the illusion that the plan grasps everything that is going on and therefore can be trusted. As a result, when you have a plan, you tend not to look for things that disconfirm it. Plans are the opposite of gossip in that they lure us into the trap of overlooking the unexpected. They also deceive us into thinking that we know more than we do. The worst aspect of plans is that they heighten the tendency to postpone action when something unexpected happens. People do nothing while they stand around asking themselves, "What was I supposed to do in this kind of emergency?"

I learned this lesson while watching some training at a nuclear power plant. This particular firm had a mock-up of a control room where they trained people, and they were very proud of the fact that it was such an accurate copy of the real thing. And it was great—a real knockout. But the unanticipated consequence of the verisimilitude is that when people got out of the training facility and went into the actual control room, they were hesitant to deal with emergencies. In one instance when something went wrong, employees waited for a long time before taking action. They just sat there, searching their memories for where they had seen this situation before in the training session. And it was the very fidelity of the mock-up to the real control rooms that caused their delayed reactions. Meanwhile, the reactor was getting hotter and hotter and hotter. The company would have been better off if its employees had only had a few guidelines, just enough to keep them moving in times of crisis.

All this is not to say that plans are unimportant in organizations. They are important, but not for the reasons that people think. Plans are signals, games, excuses for interactions; they are not good for micromanaging the unexpected.

You've said companies need to encourage their employees to "galumph." What is that, and why is it important?

It doesn't match the dictionary's definition, but I use the term to mean a kind of purposeful playfulness. It is not frivolous or aimless play but a kind of improvisation whereby organizations try out different possibilities. In this sense, galumphing keeps people from becoming too complacent; it helps executives see things in a new way. Consider wildland firefighters: Did you know they are most likely to get killed or injured in their tenth year on the job? That's just about the time they start to think they've seen it all. They've adapted extremely well to past challenges but have become less open to new information that would allow them to adapt to new challenges. That's why firefighters, like people in other organizations, should constantly be encouraged to imagine different possibilities.

In wilderness fire training, for example, it is crucial to learn how to escape from flames when you are in danger of entrapment. One way to do this is to drop your tools so that you can pick up speed. The problem is, it feels very unnatural to firefighters to drop their tools—for them, it is almost like losing their identities. In very recent training, therefore, firefighters play at dumping their packs; they explore what it feels like to run both encumbered and unencumbered. The crucial point in this exercise is that firefighters learn not to take things for granted. If they understand that survival literally depends on the ability to see things differently, they will learn to be more mindful. It's the same for executives: Galumphing helps them enlarge their repertoires and gain confidence in alternative ways of acting. It is particularly critical in high-reliability organizations, where the last thing anyone wants is for people to let down their guard because they think they've seen everything.

A version of this article appeared in the April 2003 issue of *Harvard Business Review*.

---

**Diane Coutu** is the director of client communications at Banyan Family Business Advisors, headquartered in Cambridge, Massachusetts, and is the author of the HBR article "How Resilience Works."

---

**This article is about ORGANIZATIONAL CULTURE**

 FOLLOW THIS TOPIC

Related Topics: RISK MANAGEMENT | PSYCHOLOGY | MANAGING ORGANIZATIONS | CHANGE MANAGEMENT

