Red Cross Says ‘Always Be Prepared’

When a natural disaster strikes, it leaves a trail of devastation in its wake. No matter how prepared we think we are, it’s always a shock when someone’s home, safety and family are directly impacted.

Thanks to dedicated supporters like you, American Red Cross relief teams can show up to help families recover from situations no one would ever want to face.

As disasters become more frequent and intense — as they have this past year — Red Cross volunteers are prepared to respond whenever and wherever needed. This past spring, after severe weather like tornadoes, storms and flooding wreaked havoc across multiple states, from Hawaii to Georgia, Red Cross teams sprang into action.

“I never really thought about this until I started volunteering with the Red Cross, but we are so vulnerable to lose everything in just a matter of seconds, and for the Red Cross to be there and to be able to provide that assistance, it’s just amazing.”

Pilar Cantor, a Disaster Action Team volunteer who helps families recover after disasters

While we can’t stop emergencies from happening, we can help make sure that people never face them alone. We’re dedicated to helping our communities prepare, respond and recover in the face of any disaster. You can find tips to help your family prepare for unexpected emergencies on our website.

Right now, volunteers are standing by to ensure people are cared for in the aftermath of disasters big and small. But you can take the appropriate steps today to prepare for when the next emergency strikes.

If you or someone you love is affected by a disaster, you are not alone. The Red Cross is here for you with emergency aid when you need it most. Click to find out more.

Sincerely,
Alison Teres
Executive Director, Humanitarian Services, American Red Cross
Be Red Cross Ready

It’s as easy as 1-2-3! Getting prepared may sound difficult or time consuming but – with a little help from the Red Cross – it’s actually very doable.

1. **Get a Kit**  Learn the essential supplies to put in your family’s survival kit.

2. **Make a Plan**  Plan effectively for you and your family in case of an emergency.

3. **Be Informed**  Understand which disasters are likely to occur in your area and what you must know to stay safe.

The Red Cross is proud that an average of 90 cents of every dollar we spend is invested in delivering care and comfort to those in need.

This article from the Red Cross e-newsletter. Whether you support them or not is a personal choice. We just want you all to be prepared for when ‘IT’ happens!  Bob

---

**Heat Can Be Dangerous!**

Disaster Resistant Universities (DRU) is a coalition of emergency preparedness practitioners from across the country. Dave Bujak has been helpful on several of my projects for Colorado State and offers this information about the dangers of heat. Especially if you have young and old members in your family, please look this information over. While our campus may be lightly populated for this summer, we all like to enjoy our Colorado outdoors. Do so safely please! The article is used here with Dave’s permission.

1.) FACT: Heat is the **#1** weather-related killer in the United States!

2.) Listen to the experts: visit UConn’s Korey Stringer Institute at https://ksi.uconn.edu/ to learn the most about heat’s impact on people, especially those outdoors, exerting themselves in full sun. KSI covers many key topics including:

- **Prevention:**
  - Protective Equipment
  - Wet Bulb Globe Temperature (WBGT) Monitoring
  - AED’s
  - Coaching Education
  - Hydration
  - Heat Acclimation
  - Pre-Participation Examinations
  - Emergency Action Plans
  - Sports Medicine Policies & Procedures

- **Emergency Conditions:**
  - Anaphylaxis
  - Asthma
  - Internal Trauma
  - Cardiac Conditions
  - Cervical Spine Injury
  - Heat Illness
  - Exertional Sickling
  - Hypo/Hyperglycemia
  - Hyponatremia
  - Traumatic Brain Injury
  - Lightning

- **Research**

- **Services**

- **Outreach**

- **Education**

  [Note – you can find most of these same resources by simple topic/title searches of our own Colorado State home page. . . like you didn’t already know that 😃 Bob]

3.) Know the difference between:

- **Temperature** – the raw ambient air temperature as measured in the shade absent any wind impacts.

- **Heat Index** – The measure of temperature and humidity (or dew point) as a proxy for what it “feels like” as if you are sitting still in the shade, absent any wind.

- **Heat Stress** – Scientifically known as WBGT – Wet Bulb Globe Temperature, as a measure of the total impact on a body in a state of exertion (working, training, exercising) in direct sunlight. Takes into account UV radiation, winds, etc. Unfortunately, WBGT requires either hand-held devices for on-scene measurement or some automated devices (e.g. WeatherSTEM stations) can accurately measure and approximately forecast WBGT
conditions into a user-friendly color-coded flag system (black, red, yellow, white). Where each color coincides with specific protective action recommendations. (See KSI above for more details).

4.) Realize how much acclimation plays into heat illness risk. How is it that it can be 100°F and there’s guys roofing or paving? They’re acclimated (“used to it”) and prepared. The most at-risk people are those who are “not used to it”. This is because either the heat wave came as a rapid onset relative to seasonal norms (e.g. Pacific Northwest is not acclimated to record-busting 110’s.) or they are put into a situation that don’t normally partake in (e.g. hiking the Grand Canyon as an amateur who normally takes cool strolls at the mall or big box store).

5.) Readiness: Many heat-related illnesses and fatalities result in populations that are ill-prepared or ill-equipped to manage with the conditions. This includes vulnerable populations such as the elderly or very young. This includes people hiding inside their homes with no air conditioning. Improper hydration. People need to realize when they’re at-risk and need to seek help. During high-heat events, many communities open “cooling centers” or other “cool sweep” operations like opening fire hydrants, free bus trips and entry to swimming locations, distribution of water and/or ice. Example: https://www.cityofrochester.gov/coolsweep/. We should all check on the vulnerable populations during heat waves to prevent unnecessary illness or deaths.

I hope you find this valuable and encourage you to do more research. Contact your local NWS Warning Coordination Meteorologist. If your campus is like most, your students may be gone for the summer, but you’re full of summer campers.

Dave Bujak, MPA, CEM®
Emergency Preparedness Manager
University of Rochester & UR Medicine

____________________

’IT Security for Knuckleheads’: Ten Basic Steps

by ALLAN CAREY August 25, 2010

When this article was written in 2010, the concept of “cybersecurity” was still not widely understood. Now, in 2021, the cybersecurity threat to critical infrastructure is affecting daily life for large portions of the population. Although it is generally agreed that the lack of cybersecurity is dangerous, and potentially catastrophic, many companies and agencies still lack a robust plan to protect against this threat.

Revisit these 10 common-sense guidelines to follow to protect systems and files.

Cyber security has reached a heightened level of attention both in the media and in the minds of U.S. citizens. When household names openly admit that they have been compromised by sophisticated adversaries, it gives the American public an uneasy sense of vulnerability. If it
can happen to those large organizations, the thinking goes, it can easily happen to the average person surfing the Internet as well. Beyond awareness, the media attention has also caused a significant amount of confusion not only about what constitutes a cyber threat, but also what non-government as well as government organizations and agencies should be doing to improve and protect their cyber security systems and overall readiness.

What many citizens do not fully comprehend – this generalization also applies to many senior leaders of both public and private organizations – is the level of sophistication and complexity that already has been achieved by the nation's cyber adversaries. In fact, an attacker “supply chain” has developed that is analogous in many respects to how the illegal drug industry works: One group focuses on developing malware, another is responsible for and effective in quality assurance, yet another acts as the "trusted broker" between supplier and buyer, and the buyer specializes in developing and implementing exfiltration strategies. When large quantities of data – e.g., credit card numbers, healthcare records, and other personal-identity information – are stolen, the data is broken down into smaller units and sold to groups that use the information for illegal, larcenous, and sometimes dangerous actions against private citizens and public officials alike.

Greater in-depth understanding of the global "underground" cyber economy and its participants can be found in Fatal System Error by Joseph Menn. The bottom line is that, if an organization – whether it is a government entity providing critical citizen services or a commercial enterprise – possesses valuable information, someone, or some group, will go after that information.

Advance Planning, Total Awareness & a Meticulous Attention to Detail

Despite existing in an increasingly hostile and dangerous environment, many public as well as private organizations and agencies still lack the basic fundamentals of a sound information security program. Following are 10 common-sense mandates ["IT Rules for Knuckleheads," as one observer put it] that can and should be promptly developed, and fully implemented, in almost any type of organization to help prevent and detect threats to that organization's most critical operations.

1. Accept the fact that an organization will be compromised at some time or another. This is not fear, uncertainty, and doubt, but a statement of fact – backed by industry research and

SAFETY TIP FOR HYBRID WORKING SCHEDULES

With hybrid working schedules in our near future we thought a safety tip would be in order. Though obvious, it’s so simple it’s often overlooked.

So... Whenever you’re working in your building or area alone, let someone beside your family or significant other know where you’ll be and when you can be expected home. Let them know if your daily plan changes.

This way, if something happens that you may have a medical issue or other situation that needs response or help, a co-worker can ‘checkup’ on you or call your cell OR POLICE to make sure you are OK.

Times are changing and you are your own best resource in maintaining your safety and helping your colleagues with theirs.

THANK YOU!
public datasets. There is virtually no doubt that a security breach will happen at some point in time – which means that the appropriate detection and response systems and processes must be in place – beforehand.

2. Know both the business risks and the areas where the data is stored. Before developing a security strategy, there must be a baseline of the risk posture needed, as well as conversations with management to determine what risks may be acceptable and which ones require mitigation steps. In addition, the types and amount of data on the network must be understood. Many organizations do not segment and/or compartmentalize their most sensitive information from other information that might be considered either public or at least less critical. Extra effort in this area will pay lasting dividends so that additional resources can be properly applied both to the systems themselves and to the data that matter most to the organization.

3. Using a baseline risk assessment, develop both an information security policy and the operational procedures needed to implement that policy – which should be designed to cost effectively: (a) reduce risk to the organization; and (b) ensure compliance with any applicable requirements.

4. Develop a complete inventory of every asset on the network, including the applications running on those systems. Unfortunately, relatively few U.S. organizations, public or private, now have effective asset inventory and management systems in place – despite the fact that it simply is not possible to prepare an effective defensive stance or response effort if the systems that could be potential openings to compromise are not recognized.

5. Patch vigilantly and implement effective configuration and change-management processes. Operations and systems depend on software functioning properly and being patched in a timely manner. A healthy patch-management program is one of several possible layers of defense that can help guard against known vulnerabilities.

6. Employ effective access controls – both to restrict access to computer programs and data, and to prevent and detect unauthorized access. A workable procedure for assigning user access rights and permissions should be in place, with periodic reviews of access rights and permissions scheduled, and carried out, to ensure that individual access, which should be granted based on job responsibilities, remains appropriate.

7. Use "endpoint" protection technology as another layer of defense. Endpoints – e.g., desktops, laptops, and mobile devices – are typically the main entry point for attackers and malware into a network. Much if not quite all current anti-virus technology has been commoditized and is frequently ineffective. However, most organizations have moved toward policy-enforced endpoint security suites that integrate several technologies into a single system for simplicity.

8. Develop a more effective network monitoring capability to give the network a memory. Many and perhaps most intrusion-detection and other signature-based approaches do not detect the most serious network attacks. To cope with today’s threat environment, the data will have to be not only recorded, but also analyzed for post-incident forensics and real-time situational awareness – as well as, not incidentally, for predicting potential future intrusion scenarios and the development of preventive countermeasures (similar to those used in business-continuity planning and disaster-recovery exercises).
9. Also have in place a solid incident-response plan and capability, either in-house or through an external provider, to swiftly and efficiently: (a) remediate any cyber incident; and (b) collect forensic evidence. (This step probably does not have to be mentioned to preparedness professionals, but it does have to be reinforced.)

10. Educate end-users on the risks posed by cyber threats. Also, enable them to make informed decisions when performing their jobs, and to act responsibly when using the Internet. Human error – e.g., clicking on email attachments from unknown sources, and visiting infected websites – and social engineering are quite possibly the biggest threats to an effective information security program. In ways somewhat analogous to those used in other domestic preparedness and response scenarios, users must know how to act, quickly and effectively, and react in the cyber realm.

By implementing a sound information security program, backed by an easily understood and enforceable policy, preparedness professionals and their organizations will be in a much better position to defend against cyber-attacks. Armed with both factual knowledge and operational intelligence, a level of situational awareness and confidence can be achieved to answer the truly difficult security questions such as “Did we have a breach?” and "Was there any data lost?"

Allan Carey, a Director with NetWitness, has 10 years of information-security industry experience from serving as senior vice president (research and product development) of IANS and program manager of security services of IDC. He also has been a professional advisor to several Fortune 1000 organizations, providers of security technologies and services, and various financial-community companies through in-depth market analyses, industry intelligence, and consulting.

This article found in: Domestic Preparedness

Editor’s Note: I’m one of the biggest knuckleheads in technology issues. I find that things written in the style of “…. For Dummies” are easier for me to digest. Hope they are for you readers also. No offense intended to anyone!  Bob

Housing and Dining Services Looking for Volunteers!

We are conducting a multi-agency emergency simulation event in August. We are looking for volunteers to be evaluators for the event and think that the CSU Building Proctor Program would be a good group to pull from. Depending on interest, it would be nice to have 2-6 volunteers.

The event is on Thursday August 12 from 4pm-7:30pm. The commitment would require volunteers to arrive at 3:30pm and stay until 7:30. As an appreciation for their help, we will be providing dinner at Ram’s Horn after the
event at 7:30. The event will be held in the HDS Academic Village area. If you are interested and available, please contact me by August first so we can provide more information.

Thank you,

Nicole Reed
Assistant Safety Coordinator
HDS Workplace Inclusion & Talent Management
OFFICE (970) 491.4746

If you’re interested, please contact Nicole soon. Nicole.reed@colostate.edu

This could be a great learning experience for you too! Bob

PREP is Changing to Safety and Risk Services

Since December last year changes in preparedness have been progressing here at CSU. When Bob Schur retired, a search was conducted, and Marc Barker became an Assistant Vice President to V.P. Lynn Johnson.

Tammy Hunt reports, “Under Marc’s leadership are all areas previously under PREP (University Policy Office, Risk Management, Environmental Health Services, and Central Receiving) as well as CSUPD, Clery Compliance, and Parking. The SRS website is currently under construction and will hopefully be published within the month. The Mission and Value statement is being edited to be more inclusive of all the departments currently in the Department of Safety and Risk Services. Additionally, what used to be the Policy site (opc.prep.colostate.edu) is being updated and will be published at policy.colostate.edu. Links to the policy library will not be changed as that site is not being restructured.”

An article from last December's CSU SOURCE says, “Safety and Risk Services is a new unit resulting from an organizational restructure and encompasses several departments that currently reside within University Operations, Environmental Health, Risk Management, and the Policy Office, and will incorporate the CSU Police Department and Emergency Management that currently report to the President’s Office.

This position will also have oversight for the newly formed Clery Compliance Office and serve as the University’s Chief Resiliency Officer. Barker’s first day in this new position is Dec. 21. He will continue to serve as co-chair of the Pandemic Preparedness Team and management of all future Campus Emergencies, such as the pandemic, will be the direct responsibility of this position. A search to fill Barker’s previous leadership position with the Adult Learner and Veteran Services office will begin in January.” [excerpt from Colorado State University Source]

Marc Barker also responded, “CSU’s Safety and Risk services will focus on protective measures, planning, training, and risk management philosophies that reduce the likelihood of negative outcomes when and where our campuses face vulnerabilities. I look forward to working with the entire CSU community as we move forward from the pandemic.”

WELCOME ABOARD A.V.P. BARKER!
With all that said, safety and preparedness is EVERYONE’S responsibility. Thanks for staying in touch with this publication and my personal thanks to those attending, or having attended, our emergency readiness trainings through Talent Development. I’ve been proud to be part of a multi-discipline team of professionals from across campus to present these classes. We will see some of you on July 8 for READY COLORADO STATE online!

So. . . be safe, be observant, be ready, not scared both at home and at work. Bob

For more resources visit the Talent Development Website and click on Emergency Readiness Training

training.colostate.edu/emergency-readiness-trainings

or

https://safety.colostate.edu

Ready Colorado State Newsletter is published six times each year – January, March, May, July, September, and November and distributed to subscribers. It includes information from Building Proctors, university staff and faculty, from businesses and professional groups and publications, government sources, and from other campuses throughout Colorado and Wyoming. These articles are put together by your Ready CSU Training Team, a university wide coalition of peers concerned about preparedness, safety, and YOU.
Check with your proctor to see what’s up in readiness here at CSU! Better yet, tell coworkers they can also subscribe to the newsletter at:

https://lists.colostate.edu/cgi-bin/mailman/listinfo/ready_csu_newsletter

This publication is intended to serve YOU, the folks who serve our students: if you have information that may be included here for the benefit of your colleagues, please send it to Bob Chaffee at Talent Development at this email address:

bchaffee@colostate.edu