Top Emerging Risks Include

Climate Change, Cyber

Subject: AM BestTV – AM Best: Top Emerging Risks Include Climate Change, Cyber
Date: Wednesday, March 11, 2020 8:05:29 AM

http://www.ambest.com/video/MediaArchive.aspx?lid=1068187747001&vid=6137743626001

Ransomware a large and growing problem

Publication
Date **03/15/2020**
Source: **Albuquerque Journal (NM)**

It was like a sudden punch in the gut, eliciting the feeling that things were about to get much worse before they would get better.

"An employee opened an email and introduced a virus into the system, and from there it spread like wildfire and just took over," Taos Municipal Schools Superintendent Lillian Torrez said, referring to the ransomware attack that shut down the district's computer system.

The attack in February 2019 was costly in time and money. "It was a wakeup call," Torrez said. "We don't think this can happen to us. It's just hard to believe, and when it does happen, you get this sinking feeling because you don't want to believe it.“

Torrez is not alone. Two other school districts, one university, one New Mexico city, one county and one state government agency have collectively spent millions of dollars to regain control of their computer systems after employees unknowingly opened emails containing an encrypted code that effectively shut them out of their systems.

97% of IT leaders say insider data breaches are a major concern

Publication
Date **02/19/2020**
Source: **M2 PressWIRE**

More than 500 IT leaders and 5000 employees were surveyed across the UK, US and Benelux regions.

In addition, 78 percent think employees have put data at risk accidentally in the past 12 months and 75 percent think employees have put data at risk intentionally. When asked about the implications of these breaches, 41 percent say financial damage would be the area of greatest impact, reflecting the evolution and implementation of more stringent data privacy regulations like the California Consumer Privacy Act.

The Industries Most Vulnerable to Cyberattacks – and Why

Publication
Date **06/22/2020**
Source: **Dow Jones News Service**

Manufacturing, government and retailing were behind other industries in important areas. Fewer than two-thirds of manufacturers and retailers have any cybersecurity program. Retailers were least likely to feel prepared to defend themselves against ransomware attacks. Government departments were also among the least prepared for ransomware attacks and well below average in offering cybersecurity training to their executives, as well as in identifying critical data.

Anxiety, depression and PTSD:
The hidden epidemic of data breaches and cyber crimes

Publication
Date **02/21/2020**
Source: **USA Today Online**

"Depending on who the attackers and the victims are, the psychological effects of cyber attacks may even rival those of traditional terrorism," says Dr. Maria Bada, research associate at the Cambridge Cybercrime Centre at the University of Cambridge.

Atlanta hack brings vigilance, tech improvements

Publication
Date **02/19/2020**
Source: **Dow Jones News Service**
By James Rundle

Nearly two years after a ransomware infection crippled Atlanta, scars remain even as the city works to move on from an incident that still dominates conversations about security.

Atlanta refused to pay the hackers, who demanded $51,000 in bitcoin.

Full recovery, which has cost more than $7 million, took around a year, Gary Brantley, Atlanta's chief information officer, said in an interview. For many city employees who experienced the attack, he said, the marks it left are clear.

The incident has also helped raise awareness throughout the city's bureaucracy, Mr. Brantley said, making conversations about funding and interdepartmental collaboration easier.

Many of the improvements after the attack have been cultural, Mr. Brantley said. Teams now have a sense of responsibility and attention to detail that was lacking before, he said, showing that tackling cybersecurity incidents can't just be focused on firewalls and servers. "It's just as much about the technology as it is about the people and the culture that you have in place," he said.

Companies Risk Cyberattack Paralysis Through Poor Planning

Publication
Date **03/12/2020**
Source: **Dow Jones News Service**
By James Rundle

CHARLOTTE, N.C. -- Rehearsals for what to do during a cyberattack are becoming more common at U.S. companies, but many employees still aren't taking them seriously enough, experts say.

Speakers at the WSJ Pro Cybersecurity Symposium, held Monday, said that companies don't practice enough to adequately prepare staff. Paying lip service to so-called tabletop exercises, in which staff gather to work through scenarios and response plans, does little to help organizations react to a real attack.

"People have a false sense of security sometimes and say, 'Oh, we did a tabletop, or we did two tabletops,'" said Roy Hadley, special counsel at law firm Adams & Reese LLP.

Proper planning and preparation should help to mitigate some of the uncertainty surrounding business disruptions caused by cyberattacks or by other kinds of crises, Mr. Hadley said. This includes concerns related to the novel coronavirus epidemic, which is prompting some companies to order or encourage employees to work from home. Remote-work programs can complicate incident-response plans, particularly if communications systems are taken offline by malware.

"We have to be anticipating, from a cybersecurity standpoint and a data-governance standpoint, how we are going to deal with those unknowns, " he said. "Because the one thing that I can guarantee you is something else like [the coronavirus] will happen."

Hacker displays child pornography during school board's Zoom meeting

Publication
Date **05/09/2020**
Source: **Plain Dealer, The (Cleveland, OH)**

An unidentified hacker displayed child pornography during Thursday night's Brecksville-Broadview Heights Board of Education meeting, which occurred over a Zoom video conference, the school district said.

The hack resulted in explicit and illegal images being broadcast to members of the public for several seconds, Brecksville-Broadview Heights City School District Superintendent Joelle Magyar said in a news release. It occurred during the final question of the hour-long meeting.

Trolls exploit Zoom privacy settings as app gains popularity

Publication
Date **03/27/2020**
Source: **Guardian Web**

Working and socialising from home has brought new risks to everyday life, as webcam meetings and chatroom cocktail hours contend with privacy invasions, phishing attacks and “zoombombings” – uninvited guests abusing the popular video service to broadcast shocking imagery to all.

Public Zoom hangouts have become a popular way to spend time for isolated remote workers, who are joining calls with names such as “WFH Happy Hour” to spend time in the company of others.

But the default settings of the service are configured in the expectation of trust between participants, meaning trolls can wreak havoc. Some zoombombers have used the screensharing feature to broadcast pornography and violent imagery. Others have revelled in the opportunity for exhibitionism, while security experts have said the file transfer feature that is switched on by default could be used to spread malware.

Ransomware claims 'unsustainable' for insurance industry

Advisen Front Page News - Wednesday, February 12, 2020
By Chad Hemenway, Advisen

SAN FRANCISCO—The “extreme rise” in ransomware attacks, and an increase in demands, are at an untenable level, said John Coletti, chief underwriting officer – Cyber and Technology for AXA XL, here at Advisen’s Cyber Risk Insights Conference.

“Something has to be done,” Coletti added. Ransomware demands that were once thousands of dollars are now tens of millions of dollars, he said.

“It’s unsustainable,” Coletti said. “You get in a situation where you get a demand for $10 million on a Friday and you’ve paid your limit by Monday – without any recourse. You don’t look good to your bosses when you’ve just paid that amount of money in three days.”

Though it is not something the insurance industry wants to do, coverage will have to start to shrink if the current rapid rate in the increase of ransomware losses doesn’t stop, Coletti said.