

THE WALL STREET JOURNAL.

Critical  
Thinking  
Resource

Technology

THE WALL STREET JOURNAL.

© 2021 Dow Jones & Co. Inc. All rights reserved.

---

## About The Wall Street Journal's Critical Thinking Resource

We developed this guide to help you maximize The Wall Street Journal as a resource for your classes. You'll be able to energize discussions and engage students with tangible examples of course concepts that your students can apply in the real world. In addition, with the help of faculty partners, we've curated a special collection of our most popular and thought-provoking articles across business. For each of these readings, we provide a summary, correlation to course topics, classroom applications and questions suitable for launching discussions and conducting assessments.

Here are some of the many ways to incorporate WSJ into your courses:

- **Course Readings:** Assign articles as required reading alongside your textbook sections. For best results, include assessment questions on quizzes and exams.
- **Discussion Launchers:** Use articles to spur classroom and threaded discussions in online and hybrid courses on core concepts and current events.
- **Extra Credit:** Allow students to read optional articles and answer assessment questions for extra credit.
- **Group Projects:** WSJ is a rich source of real-world topics for group research and presentation projects.
- **Research Papers and Case Studies:** WSJ features provide timely citations for research projects.

## Subtopic: Cybersecurity

### Table of Contents

1. [Schools Struggling to Stay Open Get Hit by Ransomware Attack](#)
2. [Why Companies Should Stop Scaring Employees About Cybersecurity](#)
3. [In Battle Against Hackers, Companies Try to Deceive the Deceivers](#)

---

# Schools Struggling to Stay Open Get Hit by Ransomware Attack

**Reporters:** Tawnell D. Hobbs

**Reviewed By:** Jason D. Harry, Brown University

**Date:** November 13, 2020

**Topics:** Ransomware, Ransomware attacks, Hackers, Cybersecurity

**Link to Article:** [Click Here](#)

**Summary:** Kidnapping; ransom notes; furtive communications with the kidnapper; fear of involving the authorities; secret cash payments; tearful reunion. These are classic ingredients to many a Hollywood thriller, and now a painful storyline for organizations and their valuable data. Remote hackers infiltrate computer systems via the internet, surreptitiously encrypt or purloin all the data and then demand payment before restoring the information to its owner. If the payment isn't made, the organization can lose all their digital information forever. These "ransomware attacks" are rife. Hackers tend to focus on "soft targets," organizations that have valuable or sensitive personal data but are relatively unsophisticated and lightly staffed in cybersecurity. Sadly, these include hospitals and schools, both providing essential services that cannot be interrupted by loss of access to their records.

School districts, colleges, and universities make attractive victims for these extortionists. Accurate numbers of ransomware attacks are difficult to tally because administrators are often loath to make them public, choosing instead to switch to back-up systems (if they are lucky enough to have them) or to quietly pay the ransom and move on. Ransom amounts ranged from \$35,000 to over \$1 million across seven cases reported in the article, as districts and schools strove to protect social security numbers, birth dates, and health information of both employees and students. Even the research results of faculty are at risk. Moves to online instruction during the pandemic have increased the vulnerability of schools.

**Classroom Application:** You can use this article in a discussion on ransomware and hacking. An interesting place to start the discussion is perhaps by comparing today's internet to the storied lawlessness of the Wild West in America. Lots of economic and community activity taking place without the guardrails of policing and governing law. You can discuss if this enables the basest human instincts and frank criminality in our society to flourish. Assuming that, as a practical matter, we can expect always to be set upon by criminals. It becomes the critical responsibility of every organization to take steps to safeguard their information assets. Failure to do so is arguably analogous to a jewelry store leaving all their stock out and front door open overnight. The likelihood of loss is high. But how is this different from the information being exposed by schools if they fail to adequately prepare?

---

*cont.*

**Questions:**

1. What steps could schools take before they are attacked by ransomware?
2. Are there some types of personal information about students that schools really don't need at all, but ask for out of "habit?"
3. To the extent that some schools and districts can't afford sophisticated preparatory countermeasures, what role should central governments play in funding or providing them?
4. If you were a school administrator who wakes up to a ransomware problem, what would you do? What would you need to know to make a good decision about whether to pay the ransom? Would you involve the police, or try to negotiate with the hackers directly?
5. Since many of the perpetrators operate from outside the U.S., what kinds of international agreements might be put in place to combat the problem?

---

# Why Companies Should Stop Scaring Employees About Cybersecurity

**Reporter:** Karen Renaud

**Reviewed By:** Jason D. Harry, Brown University

**Date:** December 7, 2020

**Topics:** Cybersecurity, Hacking, Corporate cyber security, Cybersecurity Risk Management

**Link to Article:** [Click Here](#)

**Summary:** The likeliest chink in a company's cybersecurity armor is not a failed firewall or bug in the operating system— it is an insider accomplice. Not a spy or mole planted by an attacker, but rather just an unwitting employee who has let down their cyber guard. They clicked on a phishing email and gave up their login credentials. They used the same passwords for both personal and company activities. Simple, everyday lapses in an individual's cyber judgment can put the entire company at risk.

Companies routinely train their employees to be vigilant to these techniques for hacking company systems. Instilling fear is a common ingredient of this training, fear of awful things happening to them or the company, even fear of job loss. But psychologists believe that scaring people is not that effective in getting them to change their long-term cybersecurity behavior. It is more likely to evolve into a low-grade state of anxiety or mistrust, to a point where they are suspicious of the very message meant to spur vigilance. Researchers have developed a range of options that are believed to be more effective at upping employees' cybersecurity game. These include "buddy systems" (mini teams that work together on the problem), providing resources like password managers, and removing obstacles that cause employees to improvise unsafe work-arounds to get their work done.

**Classroom Application:** The article focuses on corporate settings, but many students may not have personal experience with company guidelines on cybersecurity. So, begin the discussion by querying about their personal experiences with cyber-crime: phishing emails/texts, identity theft (e.g. credit card fraud), etc. Move toward appreciating the broader implications of personal behaviors impacting a business. Have students react to the fear-inducing measures described in the article and explore their possible effects (positive and negative). Discuss the proposed alternatives and elicit commentary on the practicality and likely effectiveness.

---

*cont.*

**Questions:**

1. How would you grade your own cybersecurity hygiene? What measures, if any, do you take?
2. Where else have you encountered attempts to hack your personal information? Perhaps seemingly legitimate text messages from vendors or shipping companies that are actually phish.
3. Have you ever been duped by a “phishing” email? What happened and what can be done to prevent this in the future?
4. Has your university done any “cybersecurity training” for you? Do their efforts align more with a “fear-inducing” or “resource-providing” approach? For example, does the university email system provide mechanisms to easily report suspicious emails?
5. Describe possible effects, both positive and negative, to the fear-inducing methods mentioned in the article. Create a proposed alternative and elicit commentary on the practicality and effectiveness.
6. As you transition toward your professional future, are you prepared to improve your own cybersecurity behavior?

---

# In Battle Against Hackers, Companies Try to Deceive the Deceivers

**Reporter:** Heidi Mitchell

**Reviewed By:** Jason Harry, Brown University

**Date:** December 7, 2020

**Topics:** : Cyber Attacks, Deception Technology, Cybersecurity Risk Management

**Link to Article:** [Click Here](#)

**Summary:** Computerized interconnectedness has enabled new ways of doing business, but it has also exposed operations to criminals around the world who are just clicks away from stealing secrets, money and commercial viability. As threats of cyber damage have evolved and accelerated, businesses have erected elaborate hardware and software blockades of unauthorized access to critical systems: firewalls, encryption, authentication, and anti-malware solutions. These expensive moats and parapets are necessary to prevent easy access, but it seems that sophisticated intruders still find a way in. Some businesses have begun employing counterintuitive “deception technology” measures to thwart attacks. Allow entry to the company’s network, and then monitor for access of attractive “bait data files” that have intentionally been scattered about. When an attacker touches the bait, systems swoop in to isolate and eject them before they can access any real data. This approach is not without its own risks, as the intruder is dangerously close to actual company data. Speed of identification is key. But when coupled with other traditional protection measures, deception technology is an effective new layer of protection.

**Classroom Application:** Since the technical details of cybersecurity are highly complex and outside common experience, consider starting the discussion by seeking an effective metaphor for protecting a business against cyber invasion. Consider castle battlements, war of attrition, an arms race, and cat and mouse as possible options. Where do the metaphors break?

Have students catalog the many possible business implications to suffering a cyber attack. As consumers, we often hear about a business being hacked and losing control of its customers’ private information. But the dangers go far beyond that. Place these on a spectrum of business impact, from a relatively minor irritation, e.g. “distributed denial of service (DDoS) attack,” to an act that literally destroys the business. It is also instructive to explore the possible motivations of the intruders. Sure, it can be money. What other goals might a cyber attacker have? Competitive advantage through operations disruption, technology secrets, market intelligence, damaging personal information about executives, etc.

---

*cont.*

**Questions:**

1. Have you ever been contacted by a business letting you know that your personal information may have been compromised by a hacker? Describe what was communicated to you.
2. What types of compensation or additional services should a business offer their customers for failing to adequately protect personal data?
3. On the borderless web, how can countries effectively enforce their laws to punish bad actors?
4. Should there be limits on what companies can do to combat cyber attacks and those who perpetrate them? Perhaps take matters somewhat into their own hands. Would it be acceptable, for example, for the “attacked” to turn into an attacker? Having identified the intruder, how about unleashing a counterattack?
5. Research the biggest business cyber attacks. Organize a table of characteristics of the events, to the extent they are known or disclosed. Include the likely motivation of the attacker, impact on the business and actions taken.



**THE WALL STREET JOURNAL.**

© 2021 Dow Jones & Co. Inc. All rights reserved.