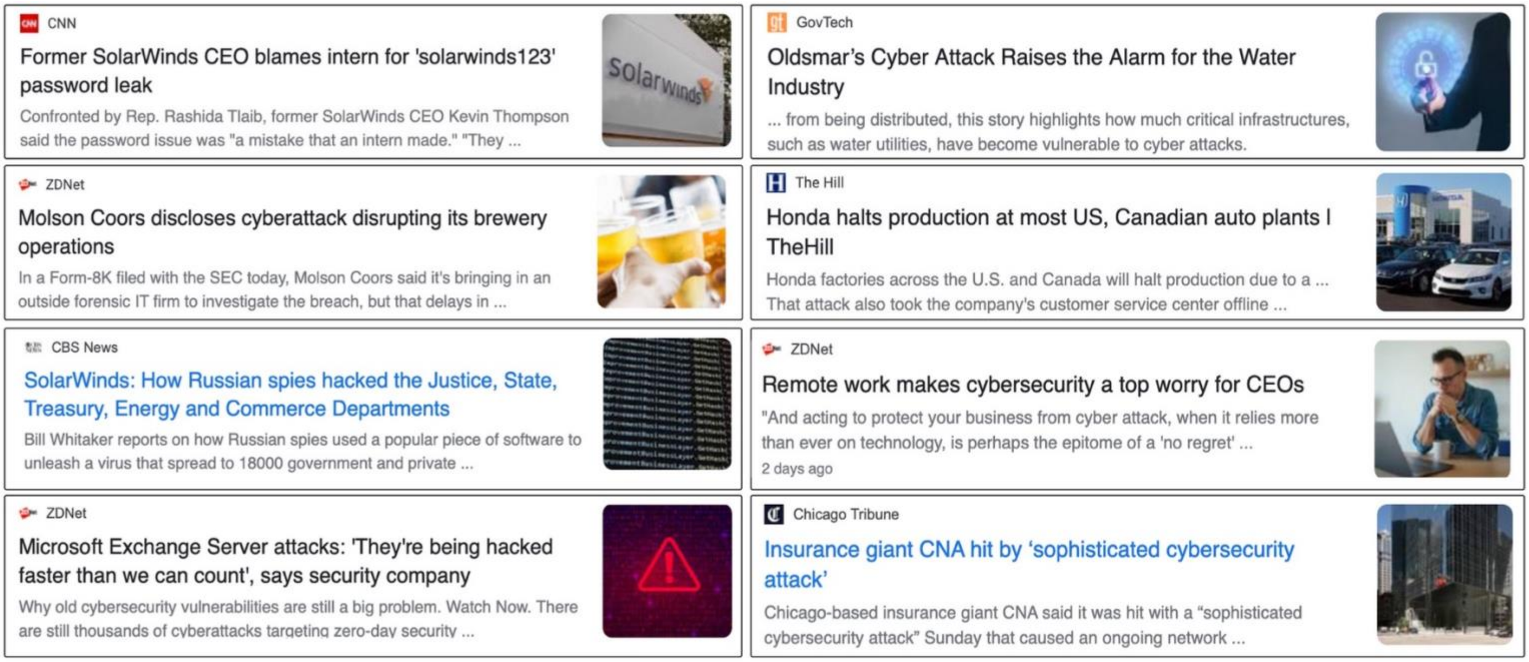
Digital Safety and the C-Suite

It's About to Get Personal

Velta Technology can help protect the C-Suite from inevitable liability relating to cyber and digital safety incidents. Gartner agrees with our view that the C-Suite is soon going to be held liable for physical security incidents due to breaches and digital missteps. By failing to take action on digital safety within their industrial environment, the C-Suite and the CEO in particular; are especially vulnerable to personal liability and accountability when a cyber incident occurs.

Gartner Predicts 75% of CEOs Will be Personally Liable For Cyber-Physical Security Incidents by 2024

"Soon, CEOs won't be able to plead ignorance or retreat behind insurance policies."



CNN
Former SolarWinds CEO blames intern for 'solarwinds123' password leak
Confronted by Rep. Rashida Tlaib, former SolarWinds CEO Kevin Thompson said the password issue was "a mistake that an intern made." "They ...

GovTech
Oldsmar's Cyber Attack Raises the Alarm for the Water Industry
... from being distributed, this story highlights how much critical infrastructures, such as water utilities, have become vulnerable to cyber attacks.

ZDNet
Molson Coors discloses cyberattack disrupting its brewery operations
In a Form-8K filed with the SEC today, Molson Coors said it's bringing in an outside forensic IT firm to investigate the breach, but that delays in ...

The Hill
Honda halts production at most US, Canadian auto plants | TheHill
Honda factories across the U.S. and Canada will halt production due to a ... That attack also took the company's customer service center offline ...

CBS News
SolarWinds: How Russian spies hacked the Justice, State, Treasury, Energy and Commerce Departments
Bill Whitaker reports on how Russian spies used a popular piece of software to unleash a virus that spread to 18000 government and private ...

ZDNet
Remote work makes cybersecurity a top worry for CEOs
"And acting to protect your business from cyber attack, when it relies more than ever on technology, is perhaps the epitome of a 'no regret' ...
2 days ago

ZDNet
Microsoft Exchange Server attacks: 'They're being hacked faster than we can count', says security company
Why old cybersecurity vulnerabilities are still a big problem. Watch Now. There are still thousands of cyberattacks targeting zero-day security ...

Chicago Tribune
Insurance giant CNA hit by 'sophisticated cybersecurity attack'
Chicago-based insurance giant CNA said it was hit with a "sophisticated cybersecurity attack" Sunday that caused an ongoing network ...

What Are You Waiting For?

- CFOs, Audit and Compliance Committee chairs share high prioritization of cybersecurity, according to KPMG.
- Cybersecurity and Infrastructure Security Agency (CISA) lists 1,200+ known OT system–related security issues, vulnerabilities, and exploits from more than 300 OEMs and system providers.
- Cyberattack and data breach incidents are predicted to occur every 11 seconds in 2021. This is nearly twice the rate in 2019 (every 19 seconds), and four times what it was in 2016 (every 40 seconds). (According to Cybersecurity Ventures)
- Ransomware damages are predicted to cost the world $20 billion in 2021, which is 57 times more than it was in 2015 ($325 million). This makes ransomware the most rapidly growing kind of cybercrime.
- The US Government DHS Industrial Control Systems Enhancement Act of 2021 is designed to strengthen the U.S. Cybersecurity and Infrastructure Security Agency, which has been tasked with securing the nation's industrial control systems and operational technology.

It's not 'if' you'll experience a breach, but 'when.'

Digital Safety and the C-Suite

Are You Asking the Right Questions?

Chances are you've asked questions of your IT team relating to cybersecurity and digital safety. It's a complicated space. How do you really know you're covered? You're getting answers, but the truth and the disconnect typically lies in the gap between your IT and Production management teams.

Below are some ***key questions*** to help you get an understanding of where things truly stand as well as ***identify any gaps*** that may exist:

1. Do we have an accurate current inventory of our plant floor assets and potential vulnerabilities? If the answer is yes, ask to see it.
2. Are we protecting our industrial environment with the same rigor as our enterprise environment?
3. Who ultimately has responsibility for protecting your industrial assets from cyber threats?
4. Have I made ***protecting*** value a priority as much as ***creating*** value?

'You can't protect what you can't see'

Fatal Digital Safety Flaws Within Most Organizations

- Assuming IT and OT (Operation Technology) departments are working closely together and have the same objectives
- Trusting Cyber insurance to provide risk protection when something eventually goes wrong
- Expecting existing staff to take on cybersecurity and digital safety responsibilities in addition to their current duties
- Underestimating employee skillset requirements and tools necessary to protect you from today's sophisticated cyber events
- Lacking visibility into Operational Technology / Industrial Control Systems on the floor that is crucial for production

Not knowing or ***being ill-informed*** won't protect you from potential liability. Be proactive rather than reactive.

We're Experts at Digital Safety and Protecting the C-Suite – Let's Talk

About Velta Technology

- Over 100 years of combined OT/ IT Industrial, Enterprise & C-suite experience
- Laser-focused on the industrial and manufacturing space
- Platform agnostic while having relationships with world-class partners across technologies & environments
- Proprietary Velta Technology Standards, Platforms & Methodologies
- Specialized Digital Safety / Cybersecurity Training program
- First to the market with Digital Safety as a Service
- Unique capabilities to put all the pieces together for a solution of value
- Qualified to exist on the production floor and in cyberspace - safely