Reducing Reputation Risk for Cybersecurity Incidents

A Follow-On to S4 in Miami | March 2024

DSTREET

Changing Public Awareness on Cybersecurity: From Consumer Data to Operational Threats

2011 – 2014

PlayStation Network

THE HOME DEPOT

yahoo!

TARGET

2015 – 2017

EQUIFAX

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

AshleyMadison's shoddy security protocols before it got hacked violated privacy laws, according to a new report released Tuesday. (Lee Jin-man/The Associated Press)

experian

Uber

MARRIOTT

BRITISH AIRWAYS

2018 Forward

MGM RESORTS

CLOROX

solarwinds

COLONIAL PIPELINE CO.

Some notable cyber-physical threats

2010 ? Stuxnet

Developed by America's National Security Agency, working in conjunction with Israeli intelligence, the malware was a computer worm, or code that replicates itself from computer to computer without human intervention. Most likely smuggled in on a USB stick, it targeted programmable logic controllers which govern automated processes, and caused the destruction of centrifuges used in the enrichment of uranium at a facility in Iran.

2013 ? ♂ Havex

Havex was designed to snoop on systems controlling industrial equipment, presumably so that hackers could work out how to mount attacks on the gear. The code was a remote access Trojan, or RAT, which is cyber-speak for software that lets hackers take control of computers remotely. Havex targeted thousands of US, European, and Canadian businesses, and especially ones in the energy and petrochemical industries.

2015 ⚡ BlackEnergy

BlackEnergy, which is another Trojan, had been circulating in the criminal underworld for a while before it was adapted by Russian hackers to launch an attack in December 2015 on several Ukranian power companies that helped trigger blackouts. The malware was used to gather intelligence about the power companies' systems, and to steal log-in credentials from employees.

2016 ⚡ CrashOverride

Also known as Industroyer, this was developed by Russian cyber warriors too, who used it to mount an attack on a part of Ukraine's electrical grid in December 2016. The malware replicated the protocols, or communications languages, that different elements of a grid used to talk to one another. This let it do things like show that a circuit breaker is closed when it's really open. The code was used to strike an electrical transmission substation in Kiev, blacking out part of the city for a short time.

COMPUTING

Triton is the world's most murderous malware, and it's spreading

The rogue code can disable safety systems designed to prevent catastrophic industrial accidents. It was discovered in the Middle East, but the hackers behind it are now targeting companies in North America and other parts of the world, too.

And so many more each year.

We now live in a world where significant cyber events happen nearly daily.
https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Outcome: High-Profile Events

- **Increased Scrutiny from External Audiences**

- **New Legislation and Acts**
  - President Biden's Executive Order 14,028 on Improving the Nation's Cybersecurity
  - The Bipartisan Infrastructure Law
  - Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022
  - The TSA/Department of Homeland Security (DHS) Cybersecurity Directive

- **And the latest…**New SEC Requirements through 8-Ks

- **Continuing trend toward disclosures**, certifying compliance ahead of time.

- **More use of cybersecurity preparedness** as a determinant of credit rating, access to capital, insurance, and other decisioning.

- Ultimately, **a significant competitive advantage for companies**.

SEC 8-K: What is Material?

Both qualitative and quantitative measures are addressed. The SEC stated in its recent ruling that the following factors must be considered when weighing the potential materiality of cyber incidents:

- The importance of any compromised information
- The impact of the incident on the company's operations
- The nature, extent and potential magnitude of incidents as they relate to any compromised information or the business and scope of operations
- The range of harm that such incidents could cause including harm to a company's:
  - **Reputation**
  - Financial performance
  - Customer and vendor relationships
- The possibility of litigation or regulatory investigations or actions including regulatory actions by state and federal governmental authorities and non-US authorities.

SEC 8-K: What is Material?

Quantitative

Quantitative factors are Primary Losses and have been referenced by the SEC in the past as follows, “Quantitative materiality assessments often are made by comparing adjustments to revenues, gross profit, pretax and net income, total assets, stockholders' equity, or individual line items in the financial statements.”

Qualitative

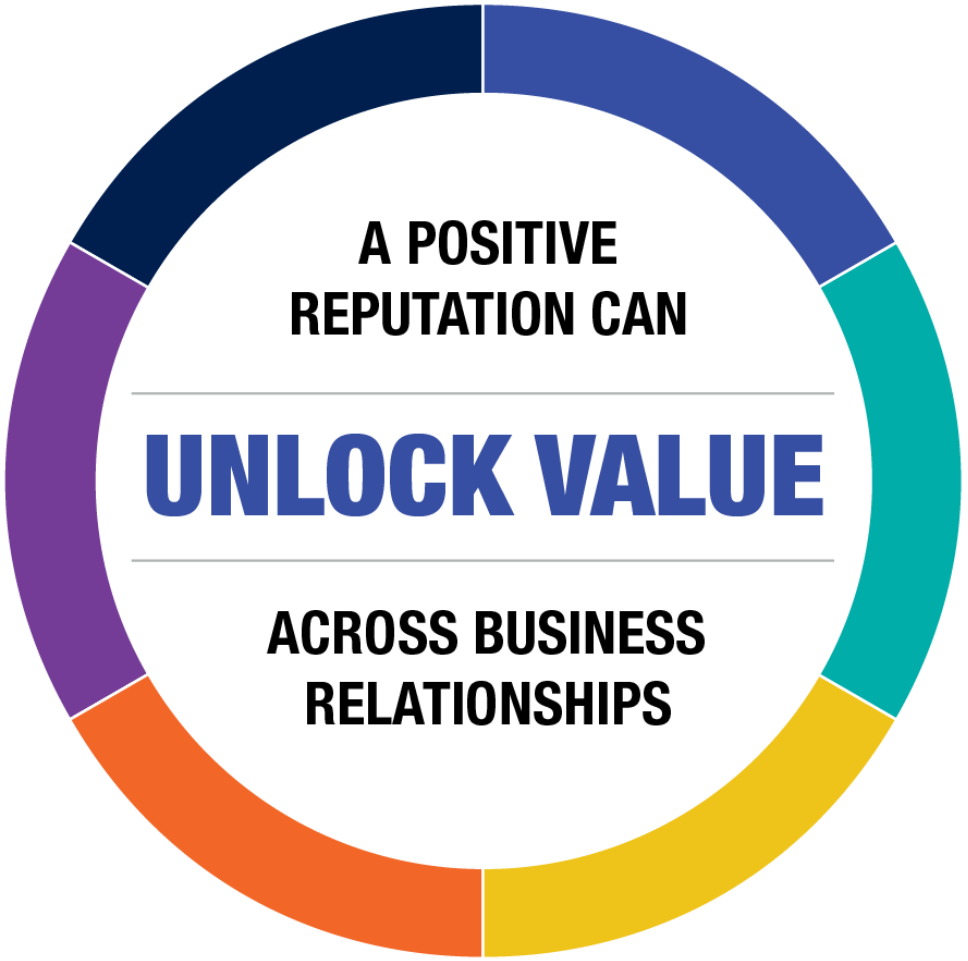
- Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, the SEC's recent ruling, stated, “The rule’s inclusion of “financial condition and results of operations” is not exclusive; companies should consider qualitative factors alongside quantitative factors in assessing the material impact of an incident.”
- The SEC further defined Qualitative factors as follows:
- **“By way of illustration, harm to a company’s reputation, customer or vendor relationships, or competitiveness may be examples of a material impact on the company. Similarly, the possibility of litigation or regulatory investigations or actions...”**

What Does Reputation Drive?

Regulatory/Policy
Fewer Headwinds:
Support for license to operate

Consumers
Equity Flow & Marketing Efficiency:
Trust in a company can strengthen trust in its brands – increasing consideration and loyalty

Financial Community
Investor Confidence:
Share price resilience and growth



Media
Communications Credibility:
A voice that is heard

Employees
Engagement:
Motivated employees delivering high performance

Business Partners
Productive Collaboration:
Supplier relationships, joint ventures, etc.

Source: IPSOS

How Important Is Reputation?

2012

A World Economic Forum study estimated reputation accounted for more than **25% of a company's market value.**

2020

In Weber Shandwick's report, "*The State of Corporate Reputation in 2020: Everything Matters Now,"* global executives attributed **63% of their company's market value** to their company's overall reputation.

Outperformance

Research from Deloitte also shows that trusted companies outperform their peers by up to **400%**.

Additional Benefits

Reputation shows up on the balance sheet as "goodwill."

Executives noted the top three benefits of a strong corporate reputation:

- customer or client loyalty
- competitive advantage
- better relationships with suppliers and partners

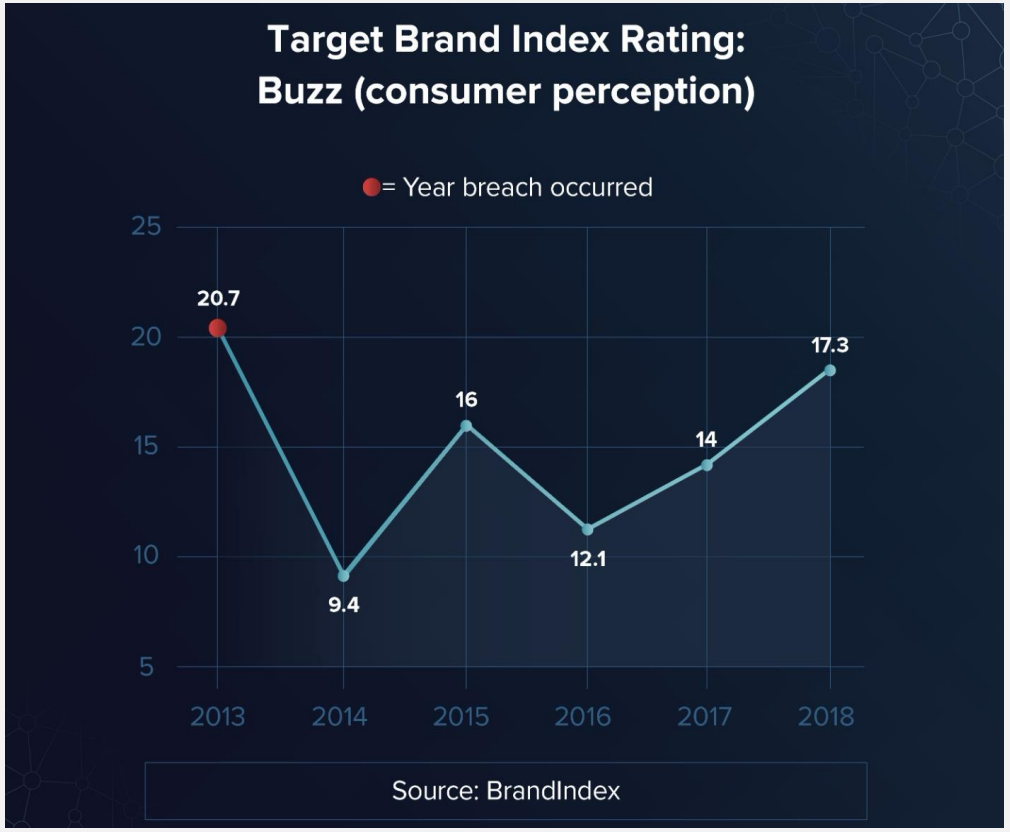
Research highlights from recent years reinforce the recognition that reputation **is not just a soft metric, but a concrete asset with measurable returns on investment** that come from managing it well.

Reputation is Affected by Numerous Areas

- **Financial Performance**
  Shareholders, investors, lenders, and many other stakeholders.
- **Quality**
  Willingness to adhere to quality standards. Product recall has an adverse effect on reputation.
- **Innovation**
  Firms that differentiate themselves from their competitors through innovative processes, and unique/niche products tend to have strong name recognition and high reputation value.
- **Ethics and Integrity**
  Firms with strong ethical policies are considered more trustworthy in the eyes of stakeholders.
- **Crisis Response**
  Stakeholders keep a close eye on how a company responds to difficult situations. Any action during a crisis ultimately affects a company's reputation.
- **Safety**
  Strong safety policies affirm that safety and risk management are top strategic priorities for the company, which builds trust and value creation.
- **CSR**
  Actively promoting sound environmental management and social responsibility programs helps create a reputation ‘safety net.’
- **Security**
  Strong infrastructure to defend against physical and cybersecurity threats helps avoid security breaches that could damage a company's reputation.

Source: Digital leadership, ethics, and challenges; Gordon Bowen, in Strategy, Leadership, and AI in the Cyber Ecosystem, 2021

Can Reputation — and Damage — Be Measured?



1 **IPSOS Global Market Research Firm**

The Ipsos Reputation Council produces a 24-country Global Reputation Monitor report.

2 **Edelman Global Communications Firm**

Regularly studies trust and reputation and produces an annual trust barometer.

3 **The FAIR Institute**

Publishes an informational website with a standard for estimating loss from a cybersecurity incident. It is aligned to the SEC requirements for reporting Materiality on Form 8-K and it addresses reputation as an element of materiality.

VISIT HOWMATERIALISTHATHACK.ORG

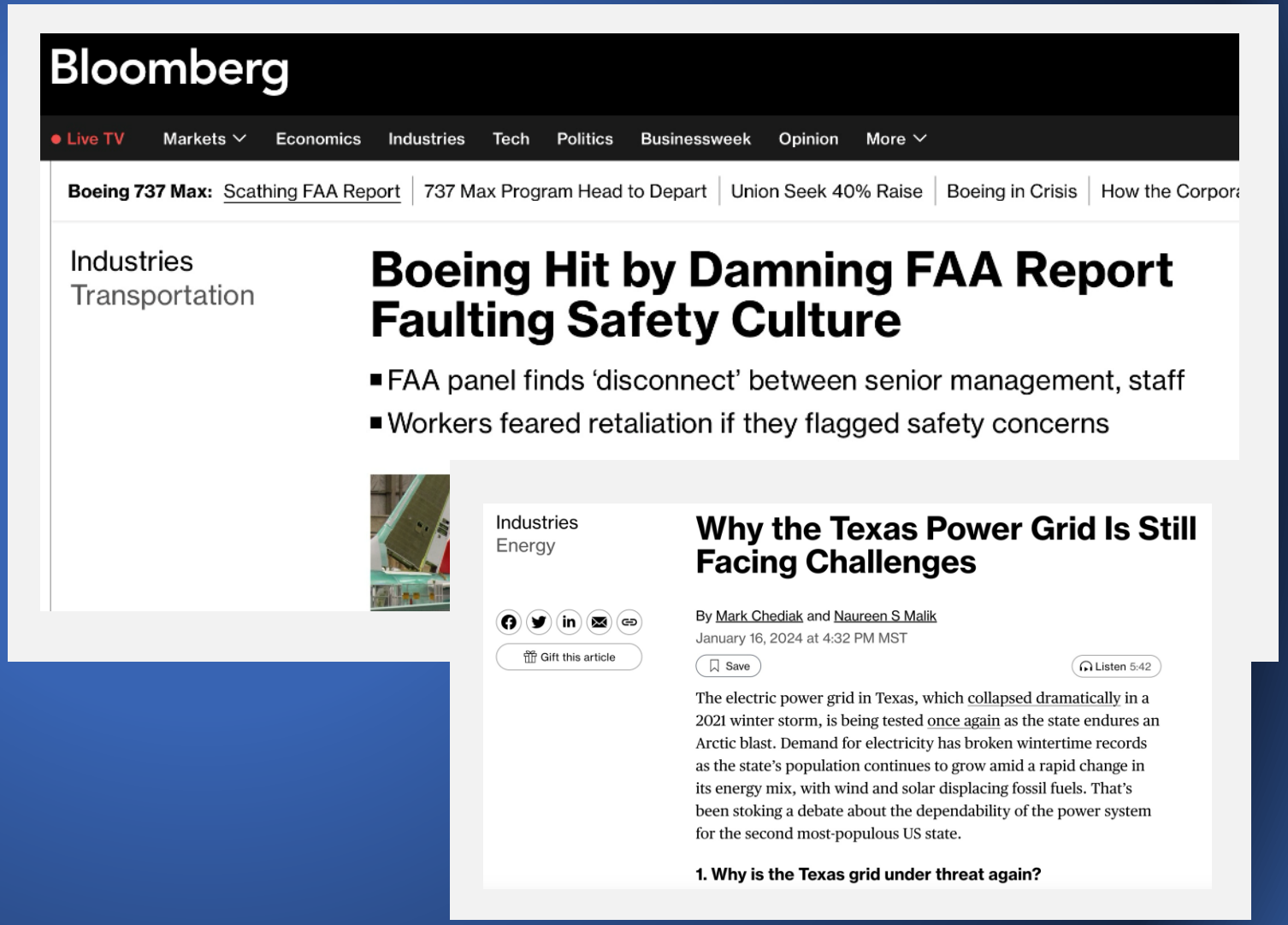
What is Reputation Risk?

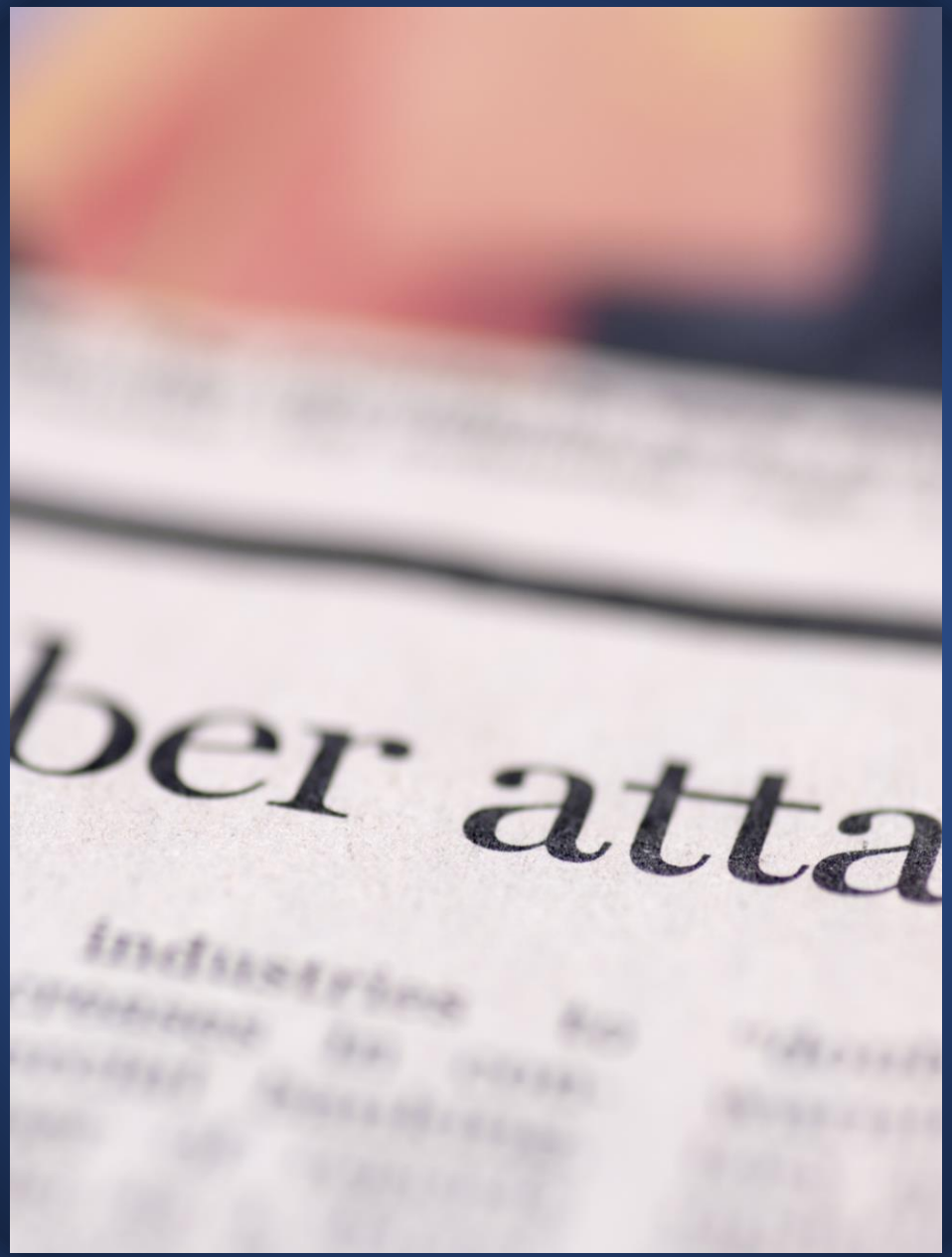
- The FAIR Institute defines it as…

  Losses resulting from stakeholder belief that an organization's value has decreased and/or that its liability has increased.

- When the brand promise fails to be aligned with the brand reality, the organization suffers reputational threat and harm.

- If you are building trust, you are building reputation. Trust is intuitively the ideal for which companies aim.





Reputation Fallouts

Enormous Expense

- In 2022, the global average cost of a data breach reached $4.35M, while the number is more than double in the U.S., averaging $9.44M.

Limiting Ability to Maintain Market Position

- These costs above can be passed on to customers and investors, limiting a company's ability to maintain its market position. For example, 60% of organizations that have experienced data breaches have raised their prices.

Underperformance

- On average, companies experiencing a significant data breach incident underperform the NASDAQ by 8.6% after one year, and this gap can widen to 11.9% after two years.

Credit Rating Downgrades

- Cyber risks can result in a credit-rating downgrade, impacting a company's ability and cost to secure financing. Moody's announced in 2018 that it would evaluate companies' cybersecurity practices when assigning credit ratings. In fact, Moody's reduced Equifax's credit rating in 2019 following Equifax's data breach that occurred in 2017.

Estimated Losses Reported

NotPetya	More than $10B in total damages
MARRIOTT	$2B in fines and legal expenses
EQUIFAX	$1.4B
yahoo!	$470M
CLOROX	$356M
TARGET	$300M
THE HOME DEPOT	$171M
PlayStation Network	$171M
Uber	$148M
solarwinds	$90M estimated insured losses; $3.5M in incident investigation, remediation, and legal fees.
MGM RESORTS	$4M - $8M a day for over a week
BRITISH AIRWAYS	$20M for fines alone

Trends and Drivers of Response Today

- **8-Ks and increased requirements for transparency offer more opportunity for misalignment between what was claimed — and what was experienced** in an event.

- **Speed continues to be a driver**, meaning you must have already established, already tested communication channels and teams with both authority and agility to make decisions in the face of an attack. **Communication response time — and services offered in the wake of an attack — will matter more and more**.

- **Supply chain attacks increase the need to understand all possible parties you might be working with.** This is not just your event; it is often one that has upstream and downstream partners involved.

Protecting Your Reputation Before the Event

Earn Equity, Understand Ecosystem, Consensus Build

Plan for and Practice Crisis Response

1. Cross-functional Teams, Tabletops
2. Holding Statements, Prepared Material, Spokespeople
3. Development of Security Narratives
4. Crisis tools such as Social Media Monitoring; Crisis Plans Accessible; Always On Line; 1-800 #s for Impacted Communities
5. Have experts, but also ensure you have muscle-tested your response beliefs. The time to be cementing agreement or disagreement on response strategies is in tabletops, not in actual events.

Earn Equity, Understand Ecosystem, Consensus Build

But Beyond Crisis Response…Regular Ongoing PR

- 360 Map of Key Stakeholders and POCs
- Established Measurement and Listening Tools
- Outreach to Influencers within Stakeholder Groups
- Participation in State Activities, Standards Bodies
- Ongoing PR, Proactive Communication Programs about Your Organization, but Also Efforts Related to Compliance, Transparency
- Speak to Successes — Through Media Relations, Briefings with Key Influencers, Articles
- Third-Party Validation

As with the new DORA regulation, having a robust incident response program with a trusted partner is a key step in ensuring a business can disclose a security incident and comply with these new rules. Businesses cannot afford to wait for an incident to ensure compliance; at that point, it will be too late for action.

No organization is immune to a material cyber incident.

Businesses must be prepared with a strong incident response plan that has been extensively practiced, with multiple scenarios and tabletop exercises.

Related to SEC Cyber Rules

Evaluate Existing Disclosure Controls and Procedures Concerning SEC's final cyber rules to:

1. Identify relevant stakeholders and assign responsibility.
2. Review existing frameworks for escalating and analyzing cybersecurity-related data.
3. Prepare an incident response plan that incorporates materiality determinations at an early stage.
4. Design, implement and test heightened disclosure controls.
5. Train employees to recognize and escalate issues.

Protecting Your Reputation During the Event

Form 8-K Determinations

New SEC Ruling: More Aggressive Disclosure Timeframe

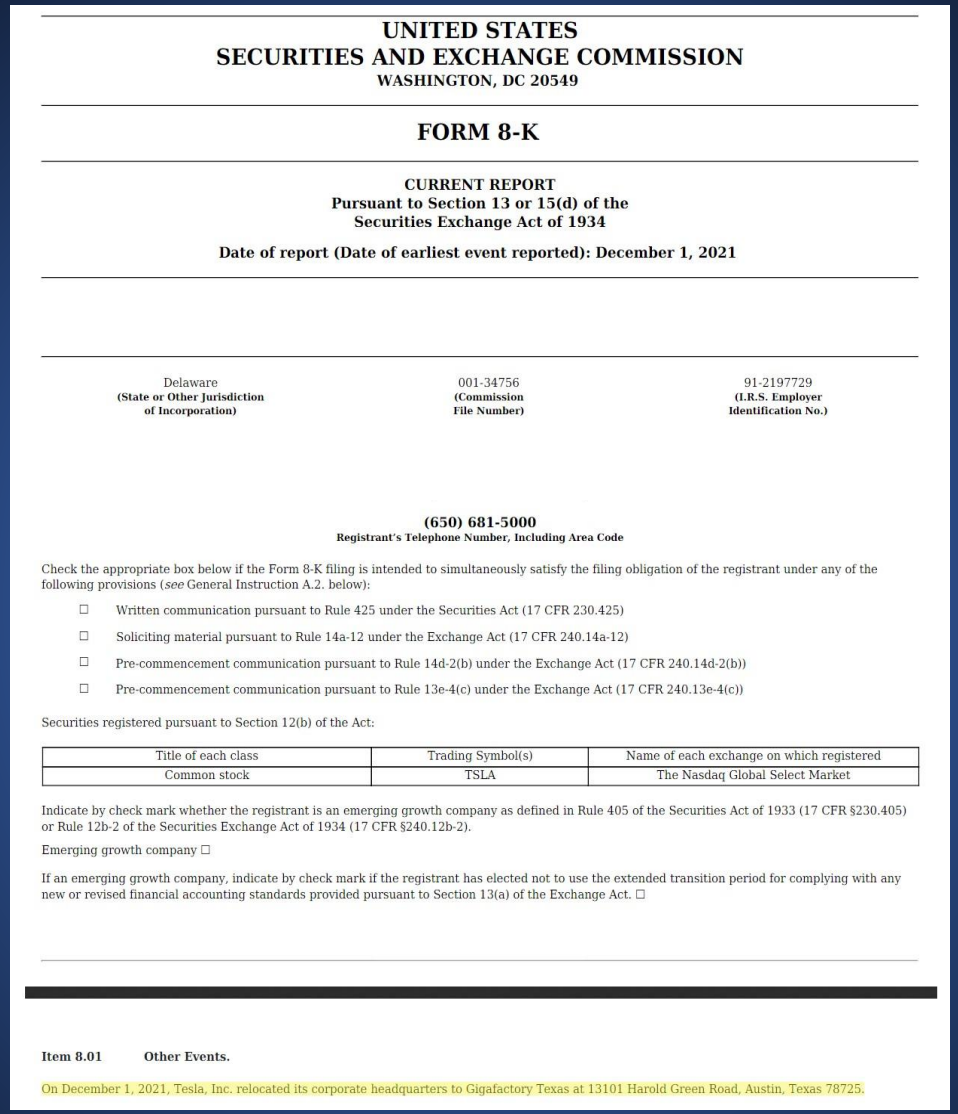
- This underscores the importance of ensuring that effective disclosure controls and procedures are in place for escalating potentially material events to senior legal and business leaders to achieve accurate and timely reporting.

Fast Assessment Required

- Companies will need to quickly determine whether an incident is material such that a Form 8-K is required, if disclosure is required, and how to ensure that it meets SEC requirements without compromising the effectiveness of its response or remediation plans.

No Detail Required That Impedes Response

- The 2023 Guidance specifically indicates that companies will not be expected to disclose specific technical information about their incident response or their cybersecurity systems, related networks, and devices, or potential system vulnerabilities in such detail as would impede their response or remediation efforts.



UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, DC 20549

FORM 8-K

CURRENT REPORT
Pursuant to Section 13 or 15(d) of the
Securities Exchange Act of 1934

Date of report (Date of earliest event reported): December 1, 2021

Delaware	001-34756	91-2197729
(State or Other Jurisdiction of Incorporation)	(Commission File Number)	(I.R.S. Employer Identification No.)

(650) 681-5000
Registrant's Telephone Number, Including Area Code

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions (*see* General Instruction A.2. below):

☐ Written communication pursuant to Rule 425 under the Securities Act (17 CFR 230.425)

☐ Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)

☐ Pre-commencement communication pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))

☐ Pre-commencement communication pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	Trading Symbol(s)	Name of each exchange on which registered
Common stock	TSLA	The Nasdaq Global Select Market

Indicate by check mark whether the registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (17 CFR §230.405) or Rule 12b-2 of the Securities Exchange Act of 1934 (17 CFR §240.12b-2).

Emerging growth company ☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Item 8.01 Other Events.

On December 1, 2021, Tesla, Inc. relocated its corporate headquarters to Gigafactory Texas at 13101 Harold Green Road, Austin, Texas 78725.

Gold Standard Responses

Operate with Speed and Agility

- Team pulling together within minutes; balance speed with accuracy

Deploy Response Strategy

- Geographic response, activation mode

Prioritize Safety and Lead with Empathy

- Human life

Take Ownership and Expect Scrutiny

- Don’t let the bad actors control the narrative due to unclear and unprepared responses from affected parties

Engage Media and Conduct Direct Stakeholder Outreach

- Activation across networks
- Focus on impacted people: Constant communication to affected customers. Call centers. 1-800 lines.

Understand 10-Hour and 10-day Window

Understanding Impact — And a Word on Empathy

1. **Map Impacted Communities**
2. **Assess Communication Channels**

In all you do, **the sanctity and value of human life must reign paramount to profits**, disrupted supply chains and inconvenience.

Yes, a crisis is a challenge for your organization to respond to, but the focus is never on you. It is not about you. It is about those impacted. **Your customers, your partners, people on the ground in the communities that are impacted.**

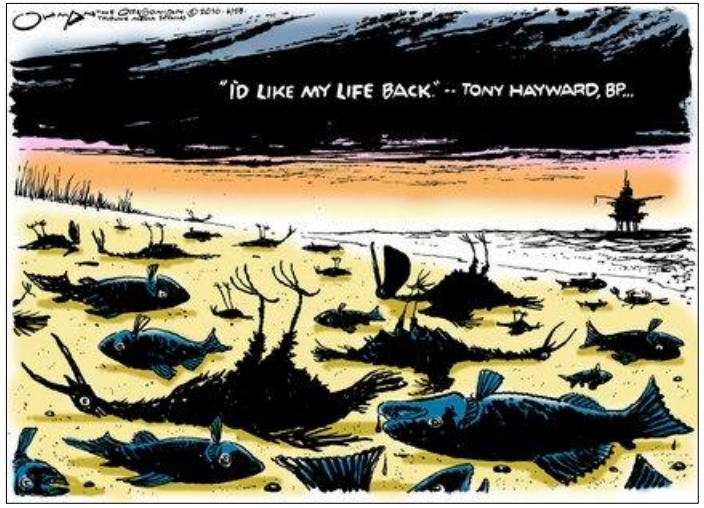
Never lose sight of this.

Spokespeople

- **Choose wisely** who can be the face of the company in an incident
- Regardless of your response, **these individuals' ability to simultaneously convey a command of the situation alongside unfolding events with empathy and concern**, will dramatically impact perceptions
- **Ensure this group of spokespeople is media trained regularly**
- **Be mindful of the visuals** coming out of the event

POLITICS

"I Would Like My Life Back," Whines B.P. C.E.O. in Ill-Advised Rant



Source: The Oregonian, 2010

Gulf Oil Spill: BP CEO Tony Hayward Apologizes For Saying 'I Want My Life Back'

BP CEO Tony Hayward Apologizes For Saying 'I Want My Life Back'

BUSINESS INSIDER

BP CEO Tony Hayward Apologizes For His Idiotic Statement: "I'd Like My Life Back"

BP CEO: His 'unbelievably callous' remark

WORLD NEWS

BP CEO on way out: Tony Hayward to get his life back; we're stuck with oil spill

Post Data Breach Reputation Recovery List

Be the **first source** to break the news

Engage in **threat sharing**

Implement a **robust notification plan**

Hire a CISO and other security professionals

Be transparent with all involved

Regularly measure and report on cybersecurity Improvements

Source: Varonis

Protecting Your Reputation After the Event

Ongoing PR and brand building are essential; coupled with government affairs, investor relations, and other efforts.

Post Event Activities

1. **Assess and Monitor Reputation Change Across 360 Map**
   - Consumer Sentiment
   - Legislative Actions
   - Partner Communications and Engagement
2. **Outreach to Influencers within Stakeholder Groups**
3. **Updates on Investigations**
4. **Address Policy Changes -** Internal and External
5. **Ramp Thought Leadership**
   - Own what happened
   - Create opportunities to lead from lessons

As the 2023 annual meeting of the World Economic Forum wrapped up in Davos, Switzerland, it ended with a disturbing prediction from one of the leading voices.

Delivering a presentation on the 2023 Global Cybersecurity Outlook report, forum Managing Director Jeremy Jurgens revealed that **93 percent** of those surveyed believe that a “catastrophic” cyber security event is likely in the next two years.

Photo Creator: Kola Shobo

In Summary

- **Public awareness of cybersecurity events that breach personal data has grown significantly in the last decade.**
- **There is growing concern from legislative and oversight bodies** — and we'll continue to see heightened interest and growing pressure to meet new requirements as a result.
- **But mainstream media is also covering cyber events that interrupt critical infrastructure**.
- **New data from Deloitte shows when it comes to business reputation, the importance of trust is at an all-time high, while the inclination to trust is at an all-time low.**

In this environment, it's clear we must remove silos, increase agility and resiliency, and regularly earn trust.

About Jennifer Dulles

https://crisisconsultant.com/

www.dstreetpr.com

Reaching Jennifer

jdulles@dstreetpr.com

Jennifer Dulles, APR

Jennifer Dulles has more than 30 years of experience advising clients on public relations and reputation management. Her clients have included tech companies including in security, IIOT and wireless technologies; large infrastructure tech providers such as CH2MHILL (now Jacobs) and TRC Companies, manufacturing companies including Schlumberger, and government and municipal entities including the US DOE and its many contractors.

In addition to founding DStreet in 2004, Jennifer serves as a senior advisor at the Institute for Crisis Management, where she regularly writes crisis communications plans and trains executive teams on effectively managing crisis.