APR 14
Jenna McNamee

The Financial Stability Board takes a stab at harmonizing cyber incident reporting protocols

Article

The news: The G20's financial agency, the Financial Stability Board (FSB), published a set of **recommendations for banks and financial authorities to create a formal process to report cyber attacks,** per Reuters.

Why is this important? The digitization of financial services has opened the door for hackers and other bad actors to steal consumers' personal information and disrupt the global financial sector with the click of a button. The FSB's framework intends to mitigate the fallout of these malicious attacks.

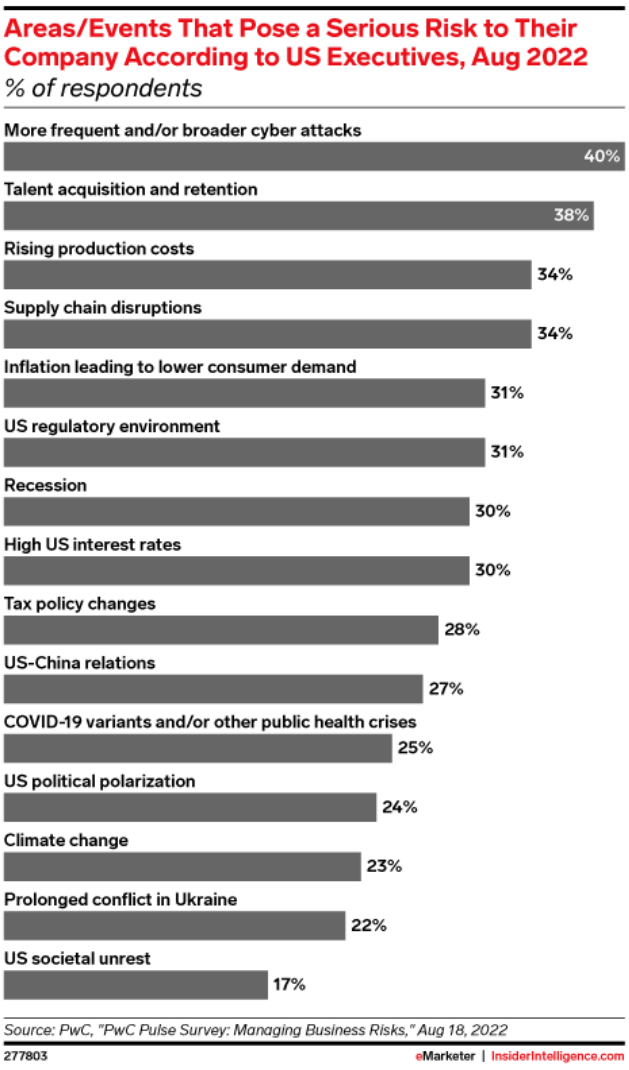
- The FSB observed that currently **there are material differences in how banks and financial institutions (FIs) report cyber attacks.** That lack of uniformity, paired with the growing interconnectedness of FIs, can accelerate spillover effects from one FI to many others.
- The agency aims to assist FIs and authorities with **creating a standard process for reporting cyberattacks** so that they can quickly implement a formal response.
- The FSB also **published an updated** "cyber lexicon" document to promote convergence in cyberattack communication and reporting.

What's the holdup? The need for standardized cyberattack reporting and formal processes for minimizing the impact of cyber attacks is clearly apparent. But the development of standards and procedures on a global scale has hit a number of hurdles.

- When a cyber attack occurs, an FI is expected to report the incident to financial authorities in its domain. This communication becomes operationally challenging when it expands to include financial regulators around the world. There's also a challenge in communicating incidents securely through a common terminology.
- Setting appropriate qualitative and quantitative thresholds at which to report an attack is difficult when dealing with FIs of varying sizes or specializing in different products or services.
- Reporting cyber attacks to all financial authorities and other FIs in a timely manner is also difficult, as an FI is likely focused on curbing the damage and mitigating the effects of an attack on its own organization.

What should banks do? The FSB has offered 16 recommendations for banks and FIs to help harmonize cyber attack reporting. Some key suggestions include:

- **Adopting common data requirements and reporting formats:** The requirements and formats should be informed by financial authorities to promote ease in information exchange.
- **Selecting appropriate incident reporting triggers:** Authorities should dictate thresholds at which FIs should report an incident.
- **Pooling knowledge to identify related cyber events and cyber incidents:** FIs and authorities should proactively share incident information so other FIs can take precautions and prevent an attack from spreading.
- **Protecting sensitive information:** Financial authorities should create safe and secure mechanisms through which FIs can communicate incidents and ensure sensitive data is protected.



This article originally appeared in Insider Intelligence's Banking Innovation Briefing—a daily recap of top stories reshaping the banking industry. Subscribe to have more hard-hitting takeaways delivered to your inbox daily.

- *Are you a client? Click here to subscribe.*
- *Want to learn more about how you can benefit from our expert analysis? Click here.*