CYBERHEDGE

Wednesday
December 4
2019

Cyber Governance Alert

informa

informa

★☆☆☆☆

12M	6M	Current
1 (▼0.66)	1 (no change)	1 (no change)

Cyber-Financial (CyFi) Analysis

- **Strategic KPI for INF's business model:** Increase market share in key segments—events & exhibitions, publishing, and intelligence.
- **How do digital assets create value for INF's shareholders?** Digital content enables company to increase events and exhibition pricing power direct to customer (exhibitor/subscription = +60% of business)
- **Biggest cyber governance problem:** A poorly protected and overly complex corporate IT network leaves primary drivers of revenue and profit highly vulnerable to a costly operational disruption via ransomware.
- **Biggest financial constraint to fix cyber problems:** Relatively high leverage on balance sheet focuses INF capital allocation strategy on paying down debt. Additional priority given to dividend payouts over improvements in security infrastructure.

Growth strategy delivers near-term results, but underinvestment in security jeopardizes medium-term performance: Informa's (INF's) aggressive growth-through-acquisition strategy has delivered on improved shareholder value and profit margin goals to date, but it has also created greater cyber vulnerabilities via an overly complex IT network and underinvestment in cybersecurity relative to the threats. Our model suggests that Informa's financial results will likely come in below expectations over the next 12-18 months if more of the currently available cash is not reinvested into better securing the company's corporate network, digital workflow assets, and hiring more security staff.

Informa has a strong portfolio of brands, the value of which are related to INF's ability to seamlessly manage large-scale events and exhibitions—a combined 61% of total revenue and 62% of adj. operating profit (H1 2019). Digitization of these workflow processes ensure greater efficiencies, leading to a lower cost basis overall.

Why Should Investors Take Note of This Alert?

The purpose of this Alert is not to predict a breach. Rather, we believe INF is more vulnerable to a potential shareholder value loss due to consistently poor cyber governance.

When considering cyber threats that could inflict the most long-term financial damage on INF, the type of breach event matters. Risks to its business are greatest if INF is hit with a ransomware attack that results in an operational disruption. When customers pay for marketing/attendance at an exhibition or event (up to 30% of a company's total annual marketing budget by some estimates), they will not tolerate operational stoppages or delays due to systems being down in a ransomware type of attack. Informa knows this since delivering "quantifiable return on delegates' investment in time and cost" is the events business core value

proposition. The company also recognizes this fact, evident in listing 'technology failure' as a primary business risk (2018 Annual Report).

But Where Have We Seen Value-destructive Events Due to Poor Cyber?

Globally, ransomware attacks are the fastest-growing form of cyber attack, and they are often timed with the dates of big logistics events because it is when victims are at their most vulnerable. The biggest attacks in recent years, such as WannaCry, Ryuk, and NotPetya, all targeted organizations with little tolerance for disruptions.

Consider the case of Boeing and the 737-Max. Regulatory standards in the aviation sector are more focused on the mechanical engineering of planes, but it turns out software engineering was the most important issue that led to tens of billions in shareholder value loss. The few security regulations that do exist globally **pertain primarily to data privacy,** while in most companies the cyber focus is on customer data loss. But **it is actually operational disruption that causes long-term financial damage to shareholders and customers**.

When Considering Financial Impact, Customer Data Loss Should Not Be the Primery Concern. In the case of INF, most would believe that customer data loss is the most likely event. In its 2018 annual report, INF management suggested it believes a data loss event is a low material risk (defined as no "Risk above 5% of EBITDA"), despite stating that a cyber breach has the highest 'likelihood' rating of the defined risks in the report.

Despite our model assigning INF our lowest cyber governance rating, we agree a data loss—based on INF's business model—would not have a material financial impact. In other words, if INF does suffer a customer data loss breach in the future, it would be embarrassing, but it has the cash to deal with it quickly and likely have insurance covering most of damages. Reputation would likely not be materially damaged because the bottom lines of corporate customers don't really suffer if their information is stolen.

The CyFi Trilemma: INF Chose Cost Savings and Growth Over Security. INF's management has proven it can meet expectations on targeted cost savings and margin expansion following the last two acquisitions. Our model is consistently finding a cybersecurity map with multiple open doors, hackers' fingerprints, and an understaffed team trying to catch up.

The below chart shows declining performance versus European media peers since July.

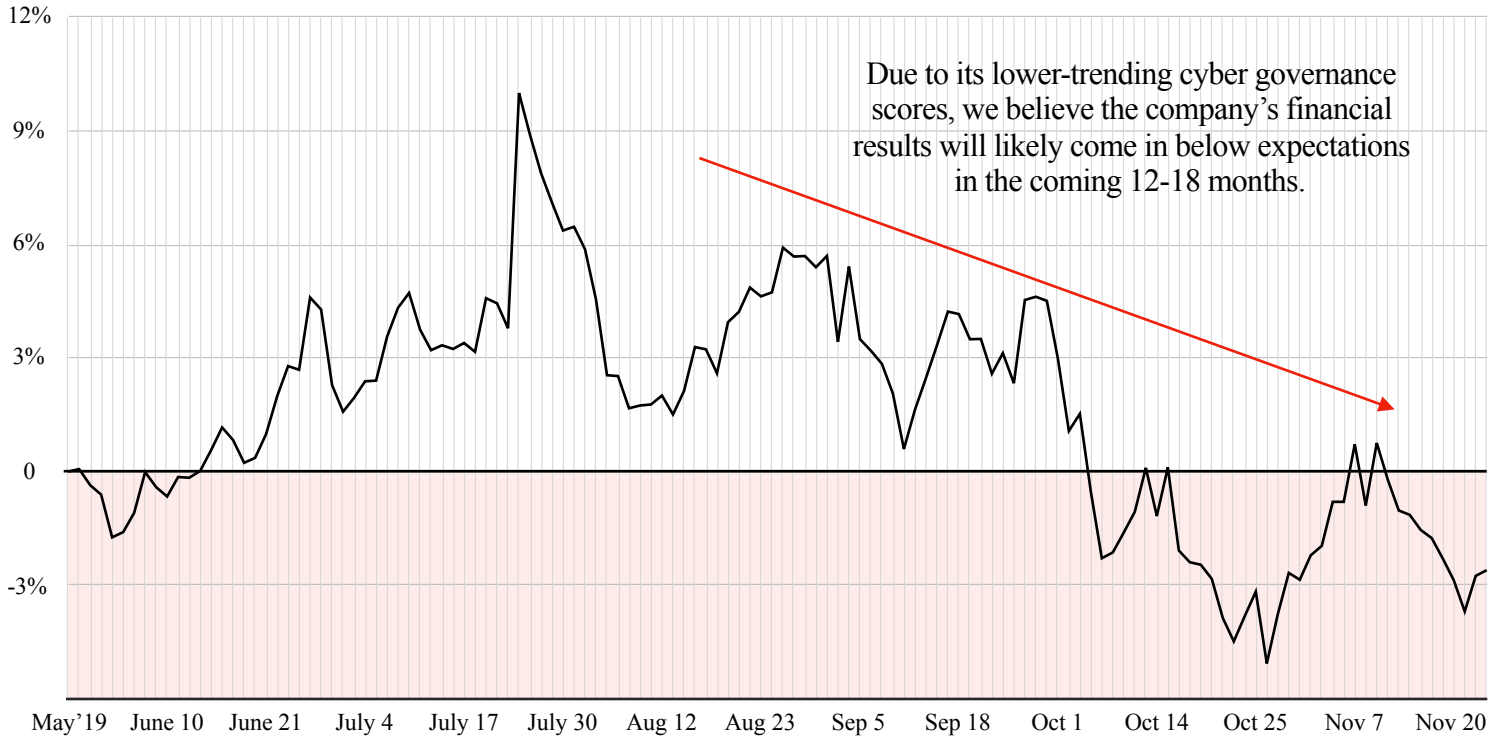

Figure 1. INF vs. Bloomberg Europe 500 Media Index

The Good News: INF has the ability to re-allocate cash to improve cyber. INF generates enough free cash flow and an impressive dividend track record (growing by 7% from 2017 to 2018) that provides management with the option to re-allocate cash to a stronger cybersecurity budget focused on more qualified staff and remediation tools. However, based on INF's investment focus on 'Brand Value' and customer acquisition tools (read: sales, not security), it's unlikely the company will be able to boost its cybersecurity budget without taking away from its investment initiatives. In light of INF management's successful integration of UBM from a branding and leadership perspective, it now might consider applying its impressive management track record now toward preventing its valuable digital workflow assets from becoming a customer liability.

Bottom Line: Though INF's aggressive growth-through-acquisition strategy has delivered on near-term improved revenue, profit margin, and share price goals, an underinvestment in technology security threatens the company's medium-term performance. Specifically, a poorly protected corporate IT network and digitization tools increase the likelihood of a costly operational disruption to two areas of the business—events and exhibitions—that currently account for more than 60% of revenues and profits. Management should consider immediate steps to improve its governance rating by addressing its overly complex corporate IT network, better protecting its valuable digital workflow assets, and hiring more security staff. If INF does not do so, its financial results will likely come in below expectations in the coming 12-18 months.

CYBERHEDGE

Cyber Governance Alert

Wednesday
December 4
2019

Research

Ryan Dodd, Founder and CEO, Cyberhedge
Chris Nolan, Senior Research Analyst, Cyberhedge
Denis Bolshakov, Creative Director, Cyberhedge

Disclaimer