# Cyber Risk In A New Era: Remedy First, Prevent Second

**September 17, 2020**

*(**Editor's Note:** This article highlights our most recent cyber insights from a credit perspective with reference to supporting case studies.)*

## Key Takeaways

- Cybersecurity is a key risk that S&P Global Ratings embeds, as relevant, in its overall assessment of an entity's creditworthiness.
- The increasing frequency of attacks and the potential for rapid deterioration in credit profiles after an attack are risk factors that are relevant for our rating assessments now.
- Leadership, communication, and external transparency are key to limiting the damage caused by a cyber attack. From a credit perspective, we believe that these factors are the most important in limiting potential rating changes post attack.
- Although it is crucial to learn from previous attacks and strengthen cyber risk frameworks in real time, the appropriate detection and remediation of attacks takes precedence as the nature of threats will continue to evolve.
- As attacks become more prevalent, entities that handle them well will ensure a better outcome, in terms of both protecting profitability streams as well as their reputation with customers.

PRIMARY CREDIT ANALYST

**Simon Ashworth**
London
(44) 20-7176-7243
simon.ashworth
@spglobal.com

SECONDARY CONTACTS

**Geoffrey E Buswick**
Boston
(1) 617-530-8311
geoffrey.buswick
@spglobal.com

**Manuel Adam**
Frankfurt
(49) 69-33-999-199
manuel.adam
@spglobal.com

**Lizzy Moir**
London
lizzy.moir
@spglobal.com

**Nik Khakee**
New York
(1) 212-438-2473
nik.khakee
@spglobal.com

**Cristina Polizu, PhD**
New York
(1) 212-438-2576
cristina.polizu
@spglobal.com

**See complete contact list at end of article.**

The COVID-19 pandemic has changed the ways we shop, learn, and work with important implications for cyber risk. E-commerce is booming, brick-and-mortar retailers are shifting to digital platforms, and schools and offices have adopted online classes and home working. For organizations, this has meant re-thinking digitalization strategies and doubling-down on information technology (IT) spending, cloud capacity, and infrastructure to boost bandwidth, ensure business continuity, and retain customers.

We believe these digitalization trends are here to stay and will inevitably lead to a higher likelihood of cyber incidents, as entities increase their digital footprint or enter the space for the first time.

The key to cyber risk resilience is a combination of risk management actions, both pre- and post attack. In this way, S&P Global Ratings expects a limited impact on ratings despite the growing number of attacks. There are a number of high profile and/or state-backed sectors for which prevention is crucial given the frequency and impact of such attacks. These may include the

utilities sectors, some financial service companies, health care providers, infrastructure, local governments, and other providers of public necessities.

However, for most corporates and financial institutions, given the importance of reputation and customer confidence within our assessment of relative credit risk, appropriate detection and risk management in the wake of an attack can be the key differentiating factor to prevent a balance sheet event from escalating to one that affects an entity's brand, reputation, or wider business profile. This risk crystalized as one factor in the downgrade of Target in March 2014 (for more information, see “Target Corp. Downgraded To 'A' Following Weak Fourth Quarter; Outlook Stable”).

The swift remediation of cyber attacks is increasingly vital, as the nature of threats will continue to evolve. Entities that do not have a well-tested playbook to help define and shape their activities following an attack will be disadvantaged and could become more exposed to future attacks. Once an attack becomes apparent, management teams have the potential to be more in control of the situation than ever before.

We believe that attacks that disrupt or inhibit operations (potentially cloud-based attacks, malware, or denial of services) may have a more meaningfully negative effect on credit ratings than those that target the theft of customer data, especially in the case of less material reputational damage or data-related regulatory fines. In such cases, the bar for swift and appropriate action is even higher to avoid negative credit rating actions.

Despite a large data breach in early 2015, U.S. health insurer Anthem Inc. was able to maintain its very strong business profile and balance sheet, resulting in an upgrade in May 2015 to 'A/A-1' from 'A-/A-2'. Anthem Inc. proactively handled the communication and policyholder redress programs in a positive manner--a crucial factor in limiting the credit implications following a large-scale attack. Our wider analysis suggests that entities that handle cyber attacks well are able to manage and maintain revenue levels in the aftermath of an attack.

## A Theoretical Cyber Risk Framework Is Only As Good As Its Performance In Practice

Companies' C-suite members remain best placed to help in-house cyber security teams engage employees in cyber prevention efforts. Employees are the first line of defense against the vast majority of potential cyber attacks. We expect management teams will be increasingly accountable for their actions or inactions on cyber. What's more, we are likely to see an increase in shareholder activist campaigns against companies that are not fulfilling reasonable standards of care in this space. In the government realm, similarly, we expect to see a weakening of constituent trust where companies do not uphold reasonable cyber prevention and response actions.

We have seen some isolated examples of cyber attacks exposing previously undiscovered control issues. Such issues can even be apparent within well-defined risk-management frameworks, especially if entities have not fully embraced desktop exercises or simulated cyber attacks as part of their efforts prior to a real attack.

For example, our downgrade of Bank of Valletta PLC to 'BBB-/A-3' demonstrated how operational risk management deficiencies, including regulatory observations and a cyber attack, increased our concerns regarding the robustness of the bank's operational risk management. (For more information, see “Malta-Based Bank of Valletta PLC Downgraded To 'BBB-/A-3' On Internal Control Issues; Outlook Stable,” July 31, 2019 and “Bank of Valletta Outlook Revised To Negative On Sharp Economic Contraction; Ratings Affirmed,” April 23, 2020.)

We believe that it would be less common for an entity to possess a strong and sophisticated cyber risk-management framework, yet still experience wider, systemic governance issues. Equally, an entity with strong governance protocols does not necessarily have robust levels of cybersecurity, but we would expect it to respond appropriately following an attack. Leadership is key in ensuring a systematic and timely response to minimize the impact, while maintaining communications with customers, suppliers, regulators, and other stakeholders. Appropriate communication channels to connect with relevant stakeholders, conveying clear and transparent messages, as well as attempting to alleviate stakeholder concerns upfront have proven to be key success factors to date.

Many of our rating criteria frameworks across different asset classes include a focus on overall governance standards and/or risk management attributes. This helps us to reflect material gaps in risk frameworks in existing credit ratings, especially where we identify operational risk-management deficiencies.

## Our Analysis Deepens Depending On The Potential Magnitude Of The Risk

For many of the entities we rate, cyber risks already constitute an important part of the operational challenges they face. We expect to increasingly focus on this risk factor as part of our management meeting discussions in the coming months and years, as the growth of cyber risks has more potential to shape credit fundamentals.

Our current focus on cyber risks scales up or down depending on the sector and the issuer-specific dynamics and exposures. If we believe an issuer is materially exposed to such a potentially material tail risk, we would seek to reflect this in the current rating.

Although we have flagged cyber security as an important risk that will affect the global credit landscape, we see certain sectors such as public finance, restaurants/retail, mainstream technology companies, and banking as being relatively more exposed. For such companies and issuers, we focus more on understanding their exposures and risk management and mitigation plans. We expect to engage and discuss more with management teams on this topic than ever before, especially to understand preventative actions as well as any cyber risk framework enhancements that are planned following attack post-mortems.

When cyber attacks occur, they are unexpected and sometimes remain undetected for many months. However, to date, they have had limited direct impact on ratings. This is mainly because of the relatively small impact on entities' balance sheets so far, particularly compared with other risks such as recent macroeconomic pressures. In addition, high-impact attacks have largely been concentrated on state-backed entities, which often allows for a wider range of potential actions and revenue bases to help in the response efforts. These institutions have, in general, demonstrated reasonable responses following attacks.

## Cyber Past Is Not A Good Guide To The Future

Cyber events and threats evolve dynamically--there is a constant battle of finding and patching system flaws, both from the perspectives of attackers and defenders. Indeed, it is a game with high stakes.

We believe there will be a tipping point within the next decade, likely accelerated by the COVID-19 pandemic, when the frequency of successful attacks increases. If this is accompanied by a simultaneous increase in the severity of an attack, there may be a more significant effect on

entities' credit profiles, especially if handled poorly. The severity of cyber attacks may be relatively low currently, but in the case of governance deficiencies and poor handling, the frequency and cost of attacks can add up (in terms of fines, brief business interruption cases, data recovery costs), potentially damaging profitability and cash and liquidity levels.

Strong balance sheets help entities to manage the cost of potential fines for non-compliance with information security regulations, compensation for customers, and, at the extreme, cyber ransom payments. Cyber insurance is proving an increasingly useful tool in transferring risks off balance sheets, but insurers will need to offer more relevant products for the market to succeed (see “Cyber Risk In A New Era: Insurers Can Be Part Of The Solution,” Sept. 2, 2020). The importance of legal and regulatory compliance has never been more important (or more complex). Entities find it close to impossible to stay fully abreast of all potential threats--limited budgets and cost controls mean that cyber spend is a finite resource. It is also difficult to demonstrate the need for cyber spending when the entity has not suffered financially following an attack. Cyber risk-management teams seeking budgetary approvals from their C-suite will fare better if they can demonstrate most "bang for their buck" for cybersecurity investments. This may be a difficult sell, but the importance cannot be underestimated and often requires a creative approach to highlight return on investment.

In the case of Travelex Holdings Ltd., for example, we placed the 'B-' ratings on CreditWatch negative following a cyber attack in January 2020. After successive downgrades to 'CCC' and then to 'CC', we subsequently lowered the rating to 'D' (default) in August 2020 following a perfect storm of cyber, governance, and financial reporting issues, as well as challenges related to COVID-19. We indicated that we saw negative pressure on the ratings in January 2020, where we cited our concerns about the strength of overall governance and internal controls. (For more information, see “Travelex Holdings Ltd. 'B-' Ratings Placed On CreditWatch Negative On Cyber Attack Disruption,” published Jan. 9, 2020.)

This example also highlights the potential impact of cyber attacks on credit ratings given how much they can disrupt operations and day-to-day functioning. This is exacerbated in the case of suboptimal protocols and communication in the wake of such an attack and even more detrimental in the case of a group with an excessive debt burden.

## Related Research

- Cyber Risk In A New Era: Insurers Can Be Part Of The Solution, Sept. 2, 2020
- U.S. Public Finance Issuers Must Be Nimble To Fend Off Cyberattacks Or They Could Face Credit Fallout, Feb. 25, 2020

## Contact List

PRIMARY CREDIT ANALYST

**Simon Ashworth**
London
(44) 20-7176-7243
simon.ashworth@spglobal.com

SECONDARY CONTACT

**Geoffrey E Buswick**
Boston
(1) 617-530-8311
geoffrey.buswick@spglobal.com

SECONDARY CONTACT

**Manuel Adam**
Frankfurt
(49) 69-33-999-199
manuel.adam@spglobal.com

SECONDARY CONTACT

**Lizzy Moir**
London
lizzy.moir@spglobal.com

SECONDARY CONTACT

**Nik Khakee**
New York
(1) 212-438-2473
nik.khakee@spglobal.com

SECONDARY CONTACT

**Cristina Polizu, PhD**
New York
(1) 212-438-2576
cristina.polizu@spglobal.com

SECONDARY CONTACT

**Irina Velieva**
Moscow
(7) 495-783-40-71
irina.velieva@spglobal.com

SECONDARY CONTACT

**Lena Schwartz**
RAMAT-GAN
(972) 3-753-9716
lena.schwartz@spglobal.com

SECONDARY CONTACT

**Etai Rappel**
RAMAT-GAN
(972) 3-753-9718
etai.rappel@spglobal.com

SECONDARY CONTACT

**Matthew S Mitchell, CFA**
London
(44) 20-7176-8581
matthew.mitchell@spglobal.com