WHEN THE GOING GETS TOUGH, THE TOUGH GET GOING

OVERCOMING THE CYBER RISK APPETITE CHALLENGE

APRIL 2018

AUTHORS
Michael Duane, Partner
Rico Brandenburg, Principal
Matthew Gruber, Engagement Manager
The scale of recent attacks and resulting media attention, supervisory pressures to upgrade cyber risk management, and the pace of technology innovation to keep up with are increasing rapidly. These factors are compelling financial institutions to have a clear understanding of the cyber risks they face, and to determine the level of cyber risk the institution is willing to accept.

An effective, measurable, and actionable cyber risk appetite (the set of statements and metrics that articulate the views of the Board of Directors and senior management about the scope and level of cyber risk the institution is willing to accept) provides institutions with a risk management capability to set and communicate strategic boundaries for cyber risk-taking across the institution.

Boards of Directors are increasingly requesting from senior management a coherent articulation of the institution’s cyber risk appetite linked to the business model and strategy, and integrated into enterprise risk management. More advanced institutions have been on the journey to adopt and use cyber risk appetite as a tool for decision making. Others are now playing catch-up. Developing an effective, measurable, and actionable cyber risk appetite is difficult, especially given the fast-changing nature of this risk and that cyber acts as a gateway to other non-financial and financial risks. The blurred boundaries between cyber and other risk types need to be conscientiously addressed as part of the risk appetite design to avoid or at least clearly understand forms of “double counting”.

In our experience, the journey of developing a cyber risk appetite is as important as the cyber risk appetite itself. Therefore, it is essential to engage senior management and the Board of Directors using a structured design approach that combines creating awareness and getting input. In so doing, it becomes clear why zero appetite is just not realistic.

“ZERO” APPETITE ILLUSION

The starting position of most Boards of Directors and senior management is still a close-to-zero acceptance of cyber risk. This essentially means the company cannot be “online,” an unreasonable position for modern businesses. As a result, it is challenging for senior management to propose an effective risk appetite that the institution can comply with given its business strategy.
As the scale and frequency of publicly reported cyber events – not to mention non-public events and near misses – continue to rise, cyber risk is becoming an ever more prominent topic for senior stakeholders across major financial institutions and their supervisors. In response, both internal and external stakeholders are expecting institutions to develop an effective, measurable, and actionable cyber risk appetite and to embed it into the institution’s decision-making processes and governance (e.g., IT spend).

A well-designed cyber risk appetite – defined here as a set of qualitative statements and associated quantitative metrics – is a powerful risk management tool for an institution. It provides senior stakeholders (especially those not buried in day-to-day operations, like the Board of Directors and supervisors) with a crisp articulation of the level and type of acceptable cyber risks for the institution, putting cyber risk on par with other, more familiar risks like credit risk, market risk, and operational risk. As a result, an institution’s cyber risk appetite can be leveraged as an anchor point to prioritize cybersecurity investments, both within cyber risk and across other risk types, to align the institution’s cyber posture to its risk appetite. When cascaded through the institution, cyber risk appetite becomes a powerful communication tool that enables cyber risk to be more tangible across business and support functions, raising awareness for cyber risk and for the need to manage it at every organizational level. Where metrics and thresholds are consistently propagated throughout the institution and linked to tangible actions, the cyber risk appetite acts as a governance mechanism to ensure rapid escalation of issues through early warning indicators.

Therefore, an effective, measurable, and actionable cyber risk appetite should be considered a pivotal element of an institution’s cyber risk management framework.
Crafting an effective cyber risk appetite is not a trivial undertaking and getting it right is hard (despite a common belief that it’s not too difficult to “write down a few statements that characterize the institution’s risk-taking capacity”). But the consequences of a poorly articulated cyber risk appetite can be significant.

Boards of Directors and supervisors continue to put pressure on senior management to define or improve the cyber risk appetite of their institution. While leading institutions have been at this for a while, many institutions are still experimenting with (and some haven’t even started) defining their cyber risk appetite. Across the financial services sector we observe four primary challenges explaining why some institutions have tried, but failed, (or haven’t even tried) to define a meaningful cyber risk appetite.

**Exhibit 1: Cyber risk appetite challenges**

- **Quantification challenge:** The industry has not yet agreed upon a standard approach to quantifying cyber risk (outside of scenario analysis for operational risk more broadly). In addition, institutions have only rudimentary cyber-related data that encompass a limited time-series. This complicates identifying metrics that can be tracked on an ongoing basis supported by historical data to define “normal” ranges.

- **Data challenge:** Given the rapidly-evolving nature of cyber risk, the relevance of historical data for the design of a cyber risk appetite is limited. Forward-looking statements and metrics are needed to enable institutions to identify potential issues before they become victims to the next headline-grabbing cyber incident.

- **Communication challenge:** Cyber risk metrics and reporting tend to be very technical and overwhelmingly detailed, especially for the Board. To ensure that cyber risk appetite is actionable, institutions need to strike the right balance between being too technical and too abstract, which is a difficult exercise.

- **Embedding challenge:** Cyber risk is far more than an IT problem. It spans people, processes, and technology. Therefore, it is difficult to design top-of-the-house risk appetite statements that are meaningful and communicable, can be cascaded to granular levels of the institutions, and can be translated into actionable business decisions.
A cyber risk appetite is more than just words and metrics. Appropriately adopted by and communicated throughout an institution, it can have tangible impact on business activity and behavior. Poorly articulated statements can cause confusion and may cause employees to take unproductive or potentially harmful actions. We generally see four main drivers of cyber risk appetite statements that can lead to unintended consequences, with cyber risk appetite not being effectively embedded in the institution. Exhibit 2 provides the drivers, lists example statements, and describes the potential impact.

### Exhibit 2: Examples of poorly articulated cyber risk appetite statements

<table>
<thead>
<tr>
<th>Potential consequences</th>
<th>Example statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Too broad and not tailored to the organization</td>
<td>We will have an effective cybersecurity program that meets or exceeds peer practice</td>
</tr>
<tr>
<td>Can lead to significant differences in interpretation across the organization, e.g., level of risk acceptance</td>
<td></td>
</tr>
<tr>
<td>May not provide clear and meaningful guidance for risk-based business decisions</td>
<td></td>
</tr>
<tr>
<td>Too specific and focused on technical details</td>
<td>We will prevent unauthorized access to any application or network</td>
</tr>
<tr>
<td>Can lead to unintended behaviours and incentives, e.g., providing privileged access rights to a larger than necessary user base to avoid frequent re-authorization requests</td>
<td></td>
</tr>
<tr>
<td>Makes it difficult to cascade the statement to lower levels of the organization as not all risk sub-types are covered</td>
<td></td>
</tr>
<tr>
<td>Too focused on controls rather than risks</td>
<td>We will maintain an effective control environment to protect our material assets</td>
</tr>
<tr>
<td>Does not describe the level or type of cyber risk the organization is willing to accept</td>
<td></td>
</tr>
<tr>
<td>May not provide a clear and meaningful guidance for risk-based business decisions</td>
<td></td>
</tr>
<tr>
<td>Too backward-looking and lagging</td>
<td>We will limit our tolerance for material (unsuccessful) cyber events</td>
</tr>
<tr>
<td>Reliance on historic data to predict future outcomes may lead to false conclusion given the fast changing nature of cyber risk</td>
<td></td>
</tr>
<tr>
<td>May provide false sense of comfort if, historically, the organization was less targeted by cybercriminals</td>
<td></td>
</tr>
</tbody>
</table>
THEREFORE, IT’S IMPORTANT TO GET IT RIGHT

Given the importance of a cyber risk appetite, the challenges in defining it meaningfully, and the consequences if institutions get it wrong, employing a structured approach is critical, starting with a commonly agreed-upon set of design principles. We have found the following principles to be useful when designing a cyber risk appetite (statements and metrics).

Exhibit 3: Building blocks for an effective, measurable, and actionable cyber risk appetite

- It has a clear link to underlying risk (with a forward-looking orientation) rather than just being a measure of performance
- It starts with a top-of-the-house articulation of Board-level expectations and is then cascaded to more granular levels of the institution
- It provides a forward-looking view of risk rather than just a look in the rear-view mirror
- It can be tracked, measured, and monitored to ensure adherence
- It starts with a top-of-the-house articulation of Board-level expectations and is then cascaded to more granular levels of the institution
- It reflects the unique risk profile of the institution, attractiveness (to bad actors), and attack surface (e.g., customers, third parties)
- It is a key element of the cyber risk management lifecycle and reflects the strategic boundaries for cyber risk-taking in the institution
- It can be cascaded down and across the institution to support business decision-making and risk mitigation (e.g., cyber-related IT investment)
- It reflects the unique risk profile of the institution, attractiveness (to bad actors), and attack surface (e.g., customers, third parties)

With these principles in mind, we believe that an effective, measurable, and actionable cyber risk appetite starts with the material cyber risk themes identified through a cyber risk identification and assessment process. A particular theme (or group of themes) is then linked to a statement that is subsequently cascaded to the different elements of the attack surface (i.e., workers, IT architecture, third-parties, customers). At that level, the statement is generally concrete enough to link metrics and thresholds designed to measure compliance with the statement. Metrics are aggregated and rolled up to the Board level using appropriate aggregation approaches (e.g., worst-off). Using this approach allows institutions to derive risk appetite statements and metrics that can be effectively translated into business decision processes to ensure that risk appetite is embedded in the institution. Exhibit 4 shows a high-level example for IT architecture.
Exhibit 4: What a good-practice cyber risk appetite looks like - IT architecture example

<table>
<thead>
<tr>
<th>Material cyber risk theme</th>
<th>Exposing material assets to malicious actors through unknown vulnerabilities due to a fast innovation cycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board-level risk appetite statement</td>
<td>“We will mitigate and limit the impact of business decisions on our cyber risk exposure”</td>
</tr>
<tr>
<td>WORKERS IT ARCHITECTURE THIRD PARTIES CUSTOMERS</td>
<td></td>
</tr>
<tr>
<td>Cascaded statement - IT architecture</td>
<td>We will embed cybersecurity in the design of technology and services, and reduce cyber risk exposure to an acceptable level before deployment</td>
</tr>
<tr>
<td>Metrics</td>
<td></td>
</tr>
<tr>
<td>Embed cybersecurity in the design of technology and services</td>
<td>Reduce cyber risk exposure to an acceptable level before deployment</td>
</tr>
<tr>
<td>Example metric: Number of high-risk applications depending on End-of-Life infrastructure</td>
<td>Example metric: Number of critical business processes with high residual cyber risk exposure</td>
</tr>
</tbody>
</table>

Impact on business decisions

- **Business strategy:** Cyber risk needs to be assessed as part of the due diligence when evaluating strategic business decisions, e.g., acquisitions, market entry. Decision makers need to consider the impact of business decisions on the organization’s cyber risk appetite, e.g., does the new business expose the organization as a whole to more or different cyber risk?
- **Product/service strategy:** The new product approval process needs to consider clear criteria to evaluate the impact of new products and services on the cyber risk exposure of the business/organization.
- **IT strategy:** All relevant IT decisions need to consider the cyber risk implications for the organization, e.g., End-of-Life strategy, infrastructure replacement. Additionally, cyber risk needs to be considered an input/driver for the IT strategy, e.g., moving to cloud services to improve cybersecurity capabilities.
- **IT development:** The application and system risk assessment needs to reflect cyber risk assessment criteria. The assessment results need to inform the type and scope of security controls required for detection and protection.

1. Theme identified through the cyber risk identification process

Linking relevant quantitative metrics to well-designed qualitative statements is important to measure the level of compliance of the institution with the risk appetite statement. Often more than one indicator is needed to adequately reflect a given risk appetite statement. The metrics selection process should ensure that (a) the metrics have a clear link to the statement, (b) data required to measure the metrics are available or can be collected in a timely fashion, (c) the metrics are measuring risk (rather than pure performance) and the design of the metrics is forward looking where possible, and (d) the metrics are simple and easy to interpret for an audience less familiar with the topic.

The limited availability of internal (and external) historic data for potential cyber risk metrics makes the calibration of thresholds challenging. Therefore, alternative calibration approaches need to be used to establish meaningful thresholds. Exhibit 5 outlines potential calibration approaches for different types of cyber risk metrics.
Changes in the external environment, the internal preparedness, or the business model can significantly impact the threshold for cyber risk metrics. Therefore, thresholds should be reviewed and refreshed at least annually, or more frequently in case of metrics that are impacted significantly by changes in external or internal factors.

But measuring alignment to the cyber risk appetite is not enough. To embed cyber risk appetite within the institution it is important to link tangible actions to cyber risk appetite threshold breaches. Actions should include a root cause analysis and a remediation plan to address the underlying problem that is discussed with senior management and the Board of Directors. The discussion in senior management and Board of Directors committees creates awareness, and ensures that remediation plans address structural issues and that management has the relevant resources to address the problem.
KEY STEPS FOR CRAFTING AN EFFECTIVE CYBER RISK APPETITE

Designing an effective cyber risk appetite for an institution starts at the Board of Directors level. Once the Board-level cyber risk appetite is established, the statements and metrics can be cascaded to lower levels of the institution. Starting from the Board of Directors, we recommend using a structured approach to designing an institution’s cyber risk appetite framework.

1. **Identify key cyber risks for the institution**
   - Articulate a cyber risk taxonomy and link the institution’s cyber risk identification outcome to the taxonomy

2. **Define the objectives and constraints**
   - Consider the broad range of constraints and associated objectives (e.g., financial, reputational, regulatory) that impact cyber risk appetite

3. **Create qualitative statements and identify metrics**
   - Define cyber risk appetite statements and associated quantitative metrics linked to the cyber risk taxonomy and threats

4. **Test the implications and consequences**
   - Review the emerging cyber risk statements and explore what the outcomes would be if these were solidified (e.g., target customer segments, changes in the use of third parties, changes in access rights, changes in controls)

5. **Calibrate metric thresholds**
   - Consider the metric type, available data, and the institution’s analytical capabilities in determining the correct approach to establishing thresholds for the quantitative metrics

6. **Define cascading approach**
   - Determine the level of organizational granularity to which cyber risk appetite statements and metrics will be cascaded – considering risk profile, business model, and structure of the overall risk appetite

7. **Define cyber risk appetite maintenance operating model**
   - Link risk appetite threshold breaches to tangible actions that allow the institution to “return to green”

Designing an effective cyber risk appetite is crucial for any institution that has exposure to the internet. Although it can be a daunting task, getting it right can deliver real value for the institution. A well designed cyber risk appetite (including statements and metrics) serves as a powerful tool for prioritizing cybersecurity investment, making sound cyber risk management decisions, and creating awareness for cyber risk across the institution.
Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

AMERICAS
+1 212 541 8100

EMEA
+44 20 7333 8333

ASIA PACIFIC
+65 6510 9700

AUTHORS

Michael Duane
Partner in the Risk & Public Policy and Digital, Technology, Operations & Analytics Practices
michael.duane@oliverwyman.com

Rico Brandenburg
Principal in the Risk & Public Policy and Digital, Technology, Operations & Analytics Practices
rico.brandenburg@oliverwyman.com

Matthew Gruber
Engagement Manager in the Risk & Public Policy and Digital, Technology, Operations & Analytics Practices
matthew.gruber@oliverwyman.com

www.oliverwyman.com

Copyright © 2018 Oliver Wyman
All rights reserved. This report may not be reproduced or redistributed, in whole or in part, without the written permission of Oliver Wyman and Oliver Wyman accepts no liability whatsoever for the actions of third parties in this respect.

The information and opinions in this report were prepared by Oliver Wyman. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisors. Oliver Wyman has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Oliver Wyman disclaims any responsibility to update the information or conclusions in this report. Oliver Wyman accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages. The report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. This report may not be sold without the written consent of Oliver Wyman.