ThreatConnect

Automated Cyber Risk Quantification Changes the Game at this Consumer Packaged Goods Manufacturer

Security and Business Leaders Collaborate to Create Actionable Risk Identification and Reporting

In 2020, eCommerce sales rose 76% YoY, which is good news for any company. Now, imagine being responsible for the security controls and reducing cyber risk for those 400 brands that made up that rise in sales. Think of all the applications and security controls needed to support every business function from selling personal care products to manufacturing ice cream.

Then picture having to inventory and rank all the applications used at 300 factory sites that deliver products to 190 countries around the world. Can you imagine what it would take to quantify and explain the cyber risk of those thousands of applications and infrastructure? Lastly, how would you collaborate with the business so they understood what it all meant in terms of financial risk and impact should a successful cyber attack occur?

At one of the world's largest Consumer Packaged Goods (CPG) companies, the central problem was that the organization's business side was unknowingly accepting a high level of cyber risk with deploying digital services and applications. They were operating without a frame of reference for the financial risk their digital initiatives created, nor did they understand what the impact would be if a cyber attack was successful.

Challenge

- ✓ Manually operationalized cyber risk quantification did not scale
- ✓ Applications created unknown cyber risk implications to the business
- ✓ Business and security needed to collaborate to bring down cyber risk

Solution

- ✓ Define the baseline cyber risk tolerance for the business for the enterprise (and lines of business)
- ✓ Create financial views of inherent, residual, and acceptable levels of risk
- ✓ Show business leaders the financial impact of changes in security controls

Outcome

- ✓ Results delivered for over 250 applications and 30 separate legal entities in less than 90 days
- ✓ C-Suite and board conversations now include financial cyber risk
- ✓ Business application owners now understand and can accept risk of control changes

Making Business Sense out of Cyber Risk

The security team needed a way to quantify what cyber risk meant in a business sense. All the typical indicators they used, such as indicators of compromise (IOCs) and CVSS scores, didn't mean much to line of business (LOB) owners. They needed to communicate security protections with context and relevance so application owners understood what cyber risk meant to their business.

In essence, they needed to provide a wake-up call to LOB owners about the financial impact and risk should an attack be successful on their systems or applications.

During this time, the company engaged with a top consulting firm to provide a framework strategy to better model strategic and operational risk. They were also looking to get an aggregated view of cyber risk across 300 or more facilities to understand how deficiencies in one manufacturing site could affect risk in another area.

This is no small task and is reminiscent of the laborious data loss prevention (DLP) projects before automation became widely available. Using the FAIR and CIS 20 cyber risk requirements, the consultant and customer teams got busy and unfortunately, most of it was manual work. Excel gurus were brought in to build risk models and the company went through the typical stages of manually quantifying cyber risk.

Typical stages of manually quantifying enterprise cyber risk include the following:

- ✓ Define
- ✓ Build
- ✓ Data Collection
- ✓ Validate
- ✓ Socialize

For this CPG manufacturer, it was a never-ending task to continually gather and update information and then, of course, everything changes. The company was spinning up new applications as there was consistent merger and acquisition activity. The company soon concluded that the manual work involved was unsustainable in the long run. After all, they had well over 2,500 applications across hundreds of brands. How could they possibly profile both the cyber and financial risk of all these applications? And how would they prioritize cyber risk across so many applications and business models?

Automaton Saves the Day...and A Lot of Heartache

One pivotal day, the company's consulting partner introduced ThreatConnect Risk Quantifier™ (RQ) to a member of the CISO's office. As he watched a demo, you could hear his mind ticking as he saw how RQ automatically did all the complex calculations and aggregation of data from both applications, breach data, and the continually changing threat landscape.

The important thing he saw was that it would allow his team to critique, rather than create, complex calculations to model security and threat scenarios. It showed them the impact and financial risk should a cyberattack be successful on a critical application.

From that day forward, the company transformed how they worked with the consultant. They stopped cranking out Excel models and moved toward helping the company implement RQ and onboarding their applications. The process became much simpler, the team could critique and then adjust the score RQ produced, if needed.

The important part was that they cut out the long, laborious, and manual effort of gathering and tabulating data in Excel spreadsheets and using business intelligence to produce results they could count on. There was no way that approach could scale fast enough to keep up with how quickly everything changed.

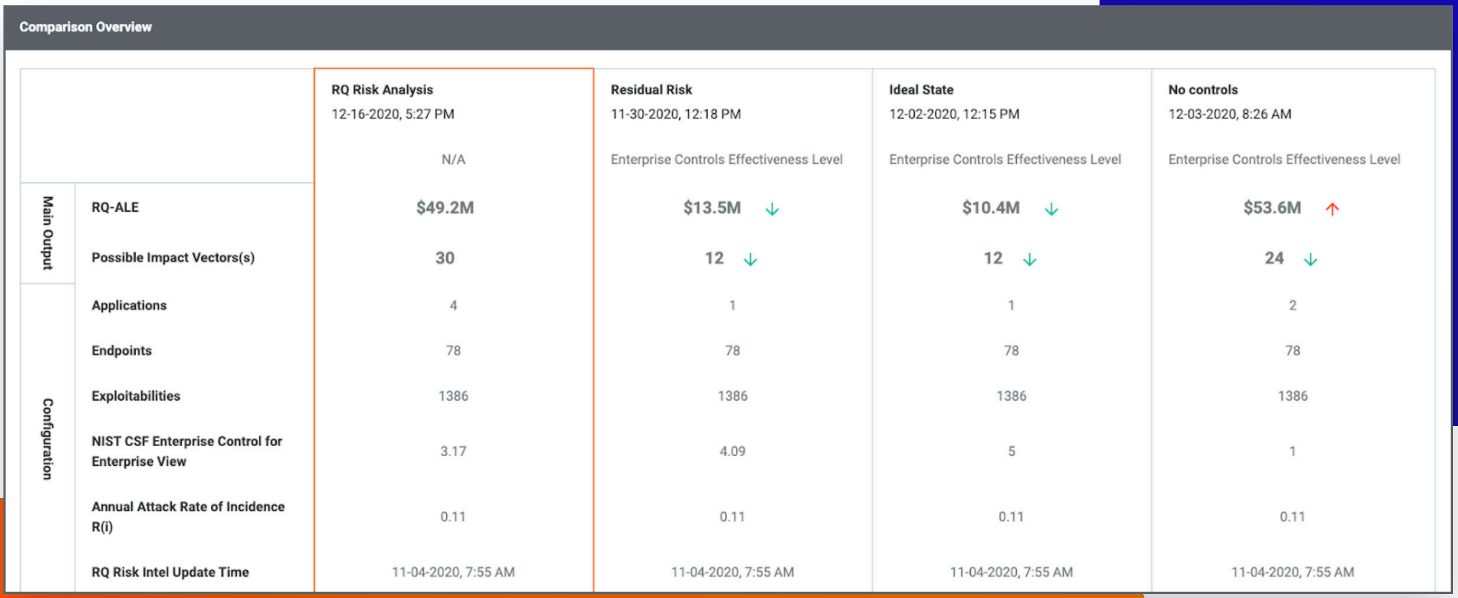
With RQ, business application owners understand risk associated with control changes and C-suite and board conversations now include financial risk. These results were delivered for over 250 applications and 30 separate legal entities in less than 90 days.

Collaboration – Not Security Policing

The conversations the company's CISO was having with other business leaders also changed dramatically. The security team never wanted to act in a policing manner with owners of LOBs. For the first time, the CISO Office could demonstrate how the lack or increase of security controls affected financial risk and impacted each LOB. Business owners who wanted waivers for security controls for their applications could now be accountable for and see the risk their decisions brought to the organization.

Finally, business owners started to understand cyber risk and wanted to work with the CISO office. No longer was there the head-butting typically found between the business and security leadership. The security team used the "What If '' Analysis capability of ThreatConnect Risk Quantifier™ (RQ) to show how different levels of security controls would affect an application's financial impact if a successful attack happened. They could run scenarios side-by-side so business owners could see how each level of security controls decreased financial risk. More importantly, it showed how having no security controls on an application increased risk exponentially.

> Finally, business owners started to understand cyber risk and wanted to work with the CISO office.



Comparison Overview

		RQ Risk Analysis 12-16-2020, 5:27 PM	Residual Risk 11-30-2020, 12:18 PM	Ideal State 12-02-2020, 12:15 PM	No controls 12-03-2020, 8:26 AM
		N/A	Enterprise Controls Effectiveness Level	Enterprise Controls Effectiveness Level	Enterprise Controls Effectiveness Level
Main Output	RQ-ALE	$49.2M	$13.5M ↓	$10.4M ↓	$53.6M ↑
	Possible Impact Vectors(s)	30	12 ↓	12 ↓	24 ↓
Configuration	Applications	4	1	1	2
	Endpoints	78	78	78	78
	Exploitabilities	1386	1386	1386	1386
	NIST CSF Enterprise Control for Enterprise View	3.17	4.09	5	1
	Annual Attack Rate of Incidence R(i)	0.11	0.11	0.11	0.11
	RQ Risk Intel Update Time	11-04-2020, 7:55 AM	11-04-2020, 7:55 AM	11-04-2020, 7:55 AM	11-04-2020, 7:55 AM

The security team was now able to explain how applications have inherent risk that will always be there and residual risk that comes from changes in security controls or application capabilities. Conversations became more collaborative as they worked together to bring down the level of cyber risk while still providing exceptional customer experience that business leaders wanted.

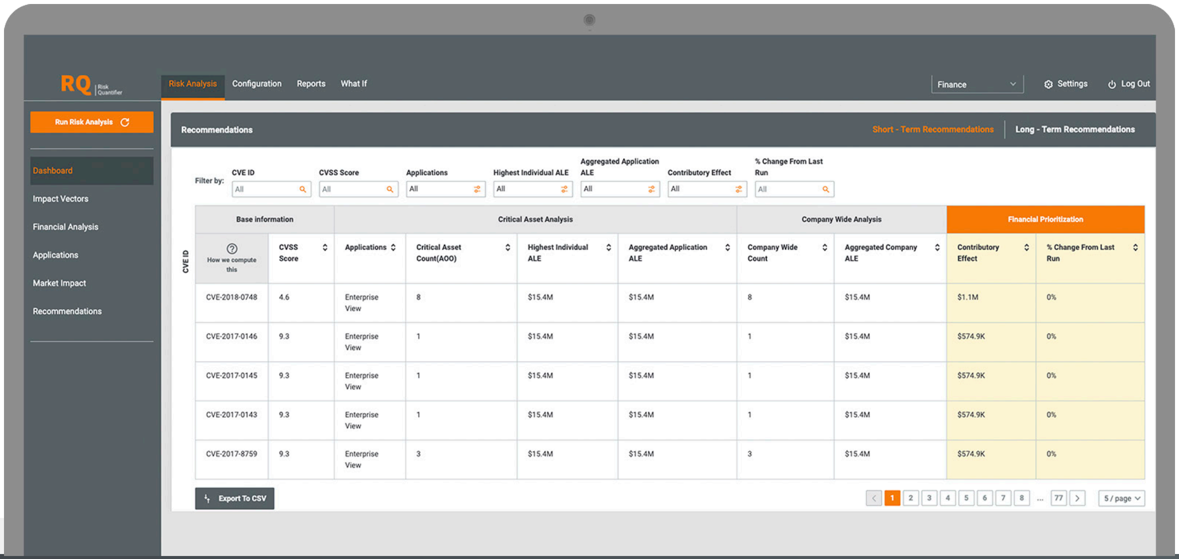
ThreatConnect

Cyber Risk Quantification Goes Global

Now that their risk assessment and quantification program's foundational capabilities are built, the team is now actively working with their consulting partner to build a worldwide program. They can now automate the generation of year-end reporting for the board and executive leadership that shows how alignment and gaps in security initiatives affect the organization's security stance compared to its risk acceptance/tolerance.

ThreatConnect Risk Quantifier™ (RQ) gave the security assessment team a way to scale thousands of applications that needed to have associated financial risk quantified. In addition, the company is collaborating with ThreatConnect to explore how to use RQ for third party risk assessment of their supply chain partners.

Within just 90 days of implementation, the team has already onboarded more than 280 applications and 41 entities. The team is continuing with plans to onboard thousands of applications over 2021.



Recommendations

Filter by: CVE ID All; CVSS Score All; Applications All; Highest Individual ALE All; Aggregated Application ALE All; Contributory Effect All; % Change From Last Run All

Base information		Critical Asset Analysis				Company Wide Analysis		Financial Prioritization	
CVE ID How we compute this	CVSS Score	Applications	Critical Asset Count(AOO)	Highest Individual ALE	Aggregated Application ALE	Company Wide Count	Aggregated Company ALE	Contributory Effect	% Change From Last Run
CVE-2018-0748	4.6	Enterprise View	8	$15.4M	$15.4M	8	$15.4M	$1.1M	0%
CVE-2017-0146	9.3	Enterprise View	1	$15.4M	$15.4M	1	$15.4M	$574.9K	0%
CVE-2017-0145	9.3	Enterprise View	1	$15.4M	$15.4M	1	$15.4M	$574.9K	0%
CVE-2017-0143	9.3	Enterprise View	1	$15.4M	$15.4M	1	$15.4M	$574.9K	0%
CVE-2017-8759	9.3	Enterprise View	3	$15.4M	$15.4M	3	$15.4M	$574.9K	0%

< 1 2 3 4 5 6 7 8 ... 77 >

ThreatConnect

Designed by analysts but built for the entire team (security operations, threat intelligence, incident response and security leadership), ThreatConnect's intelligence-driven security operations platform is the only solution available today with intelligence, automation, analytics, and workflows in a single platform. Centralize your intelligence, establish process consistency, scale operations, and measure your effectiveness in one place.

To learn more about our threat intelligence platform (TIP), Risk Quantification (RQ), or security orchestration, automation, and response (SOAR) solutions, visit ThreatConnect.com.

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com

1.800.965.2708