M&A Risk Management for a Leading Digital Media Company

DayBlink Consulting translated divestiture contractual obligations into an actionable plan and executed the plan

Introduction

A leading digital media company decided to divest a subsidiary of its business in a $5 billion deal. In addition, within the subsidiary, legacy business units were being retained that had not been previously managed. Legal obligations dictated that our client continue to provide cybersecurity services to its former business units and continue to own the cybersecurity risk in its former business units, even though the business units separately had to manage their risk from a technical perspective.

We formed the program management team to help the client reduce risk, avoid unnecessary expenses, and translate contractual obligations into tactical operations and processes that the client should implement. The client's cybersecurity team relied on DayBlink to manage relationships with the external engineering teams and deliver reporting metrics to both operational teams and executive stakeholders.

In addition, the client anticipated that it would have additional M&A activity in the future, and DayBlink's team developed materials to enable successful future risk management.

Problem

A large divestiture raised potential cybersecurity risk but our client did not have direct access to manage the risk.

Our client engaged DayBlink to closely manage technical risk that was greatly increasing due to M&A activities in a $5B deal. Our client's employees had to work on M&A activities outside of their daily job responsibilities and therefore did not have the required dedicated resources to manage the great financial risk from the divestiture. Legal requirements were broadly defined for the cybersecurity team's security service delivery. However, these requirements had not been bridged to a tactical project plan., and requirements were not clearly communicated. Day one tasks and exit tasks the Governance, Risk, and Compliance department needed to oversee were not fully discovered and well-documented. In addition, our client was newly separating from some of its previous entities but was still required to own the risk while not being able to actively manage the risk. Shortly after the divestiture, lack of engagement from the external teams, both from the executive and operational teams, started to cause breaches in contract that could have severe legal and financial impacts to both companies.

Our Guiding Principles as we developed the engagement strategy:

Clearly Defined Risk Requirements

Ensure that legal requirements clearly translate into day-to-day risk management activities and processes. Collaborate with both executive stakeholders and tactical team members to ensure work aligns with vision

Transparent Reporting

Deliver tailored reporting both upwards to stakeholders and downwards to operational teams to communicate current technical risk

Deliverables for Future M&A Activities

Develop flexible deliverable templates to ensure that client program leads are enabled to execute the program effectively for all future M&A transactions

Communications Enablement

Enable straightforward communications with internal communications channels, each dedicated to a specific purpose with the right stakeholders. In addition, add external and internal-facing channels to simplify communication with external teams

Day One and Exit Activities Support

Define highest priority activities and estimate level of effort required for teams to complete tasks. Accelerate urgent activity completion where needed, supporting both Day One and exit activities

Consistent KPI Tracking

Develop KPIs that track program improvements over time, allowing both operational teams and executive teams to isolate challenge areas and review program successes and challenges for future transaction learnings

Solution

Our team enabled risk management success through executive and operational engagement and consistent reporting.

At the beginning of program mobilization, we engaged stakeholders to collect qualitative data to discover where the program needed the most support. Initially, we collaborated with the client to solidify processes that were developed to better manage risk. This period was characterized by high turnover at our client, frequent contract analysis, and earning trust with client team members. We supported the team with building a Day One work-plan to ensure all activities were being completed as expected in a period of rapid organizational change.

As we continued to manage the program, some work streams were more mature than our client had initially expected, while others needed more attention, to the extent that active contract breaches were occurring.

We determined the client needed additional support to build relationships with technical SMEs from the separating entities, as these SMEs had the visibility and resourcing to fix the sources of the contract breaches. Delivering the necessary information for remediating and managing the technical risk was crucial in ensuring the contract breaches did not need to be escalated with legal action. Processes were built in case escalation needed to be executed to ensure external teams were prioritizing risk management.

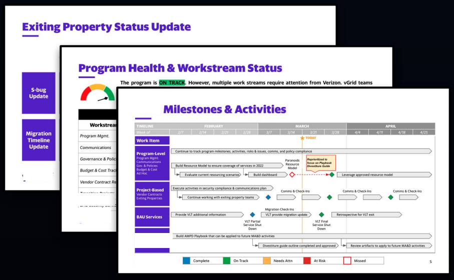
Consistent reporting to both executives and technical teams ensured leadership was aligned with our management decisions and external teams had the information to know where to focus and prioritize their efforts.

We provided project acceleration services through upfront program planning and daily project execution support with internal security teams. In addition, we presented monthly and weekly reporting to internal and external stakeholders.

Executive Reporting

Internal Only

Monthly steering committee review, weekly executive reporting, security team weekly sync



Exiting Property Status Update

Program Health & Workstream Status

The program is ON TRACK. However, multiple work streams require attention from Verizon. vGrid teams

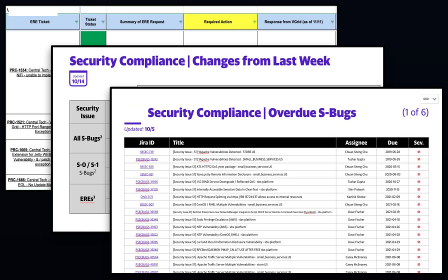
Milestones & Activities

S-bug Update
Migration Timeline Update
Workstream
Program Mgmt.
Communications
Governance & Polic
Budget & Cost Trac
Vendor Contract Re
TIMELINE
FEBRUARY
MARCH
APRIL
Week of
2/7
2/14
2/21
2/28
3/7
3/14
3/21
3/28
4/4
4/11
4/18
4/25
TODAY
Work Item
Program-Level
Program Mgmt.
Communications
Gov. & Policies
Budget & Cost
Ad Hoc
Continue to track program milestones, activities, risks & issues, comms, and policy compliance
Build Resource Model to ensure coverage of services in 2022
Paranoids Resource Model
Reprioritized to focus on Playbook Divestiture Guide
Evaluate current resourcing scenarios
Build dashboard
Leverage approved resource model
Project-Based
Vendor Contracts
Exiting Properties
Execute activities in security compliance & communications plan
Continue working with exiting property teams
Comms & Check-Ins
Comms & Check-Ins
Comms & Check-Ins
BAU Services
Provide VLT additional information
Migration Check-Ins
VLT provide migration update
Retrospective for VLT exit
VLT Partial Service Shut Down
VLT Final Service Shut Down
Build AMPD Playbook that can be applied to future MA&D activities
Divestiture guide outline completed and approved
Review artifacts to apply to future MA&D activities
Complete
On Track
Needs Attn
At Risk
Missed
5

Executive Reporting

Internal & External

Executive risk reporting spreadsheet, weekly security and compliance report, breakdown of overdue security bugs



ERE Ticket:	Ticket Status	Summary of ERE Request	Required Action	Response from VGrid (as of 11/11)
PRC-1534: Central Tech - NiFi - unable to imple				
PRC-1521: Central Tech - V Grid - HTTP Port Range Exception				
PRC-1665: Central Tech: Extension for Jetty WEB Vulnerability - & / patch exception				
PRC-1666: Central Tech - EOL - No Update Ma				

Security Compliance | Changes from Last Week

Updated 10/14

Security Issue
All S-Bugs[2]
S-0 / S-1 S-Bugs[2]
EREs[3]

Security Compliance | Overdue S-Bugs (1 of 6)

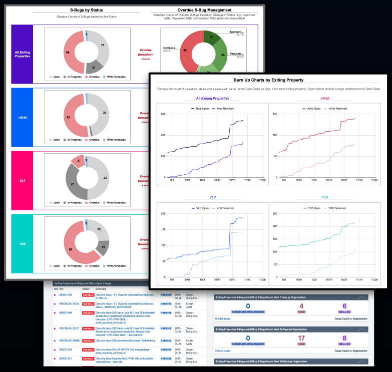
Updated: **10/5**

Jira ID	Title	Assignee	Due	Sev.
SBSEC-739	[Security Issue - S1] YApache Vulnerabilities Detected : STORE.US	Chuan-Sheng Chu	2019-05-28	S1
PSECBUGS-13243	[Security Issue - S1] YApache Vulnerabilities Detected : SMALL_BUSINESS_SERVICES.US	Tushar Gupta	2019-05-28	S1
SBSEC-836	[Security Issue S1] ATS HTTP/2 DoS yinst package - small_business_services.US	Chuan-Sheng Chu	2020-05-15	S1
SBSEC-851	[Security Issue S1] Yjava_jetty Remote Information Disclosure - small_business_services.US	Chuan-Sheng Chu	2020-08-03	S1
PSECBUGS-31856	[Security Issue S1]: ISC BIND Service Downgrade / Reflected DoS - sbs-platform	Tushar Gupta	2020-10-27	S1
PSECBUGS-33120	[Security Issue S1] Internally Accessible Sensitive Data In Clear-Text - sbs-platform	Shiv Prakash	2020-11-13	S1
ONO-3171	[Security Issue S1] HTTP Request Splitting via https://98.137.244.37 allows access to internal resources	Karthik Shekar	2021-02-09	S1
SBSEC-907	[Security Issue S1] CentOS / RHEL Multiple Vulnerabilities - small_business_services.US	Chuan-Sheng Chu	2021-02-16	S1
PSECBUGS-36569	[Security Issue S1] Red Hat Enterprise Linux NetworkManager Integration Script DHCP Server Remote Command Execution (DynoRoot) - sbs-platform	Dave Fischer	2021-02-19	S1
PSECBUGS-36349	[Security Issue S1] Sudo Privilege Escalation (AWS) - sbs-platform	Dave Fischer	2021-04-10	S1
PSECBUGS-39153	[Security Issue S1] NTP Vulnerability (AWS) - sbs-platform	Dave Fischer	2021-04-26	S1
PSECBUGS-39222	[Security Issue S1] NTP Vulnerability (CentOS_RHEL) - sbs-platform	Dave Fischer	2021-04-28	S1
PSECBUGS-39285	[Security Issue S1] curl and libcurl Information Disclosure Vulnerability - sbs-platform	Dave Fischer	2021-04-29	S1
PSECBUGS-39248	[Security Issue S1] RPCBind DAEMON PMAP_CALLIT USE AFTER FREE sbs-platform	Dave Fischer	2021-04-29	S1
PSECBUGS-40564	[Security Issue S1]: Apache Traffic Server Multiple Vulnerabilities - small_business_services.US	Casey McEnaney	2021-06-08	S1
PSECBUGS-40591	[Security Issue S1]: Apache Traffic Server Multiple Vulnerabilities - store.US	Casey McEnaney	2021-06-08	S1
PSECBUGS-40587	[Security Issue S1]: Apache Traffic Server Multiple Vulnerabilities - small_business_services.US	Casey McEnaney	2021-06-08	S1

Compliance Dashboards

Internal Only

Security bug risk management dashboard, security bug burn up chart, security bug central reporting dashboard



S-Bugs by Status

Displays Counts of S-Bugs based on Jira Status

Overdue S-Bug Management

Displays Counts of Overdue S-Bugs based on "Managed" Status (e.g., Approved ERE, Requested ERE, Remediation Plan, Extension Requested)

Burn Up Charts by Exiting Property

Displays the count of created date and resolved date since Deal Close on Sep. 1 for each exiting property. Open tickets include s-bugs created prior to Deal Close.

Exiting Properties S-Bugs and EREs / Open S-Bugs

Org	Key	Status	Summary			
●	SBSEC-739	OVERDUE	[Security Issue - S1] YApache Vulnerabilities Detected : STORE.US	OVERDUE	2019-05-28	Chuan-Sheng Chu
●	PSECBUGS-13243	OVERDUE	[Security Issue - S1] YApache Vulnerabilities Detected : SMALL_BUSINESS_SERVICES.US	OVERDUE	2019-05-28	Tushar Gupta
●	SBSEC-808	OVERDUE	[Security Issue S2] Oracle Java SE / Java SE Embedded Serialization Component Unspecified Remote Code Execution (CVE-2020-2604) - small_business_services.US	OVERDUE	2020-03-06	Chuan-Sheng Chu
●	PSECBUGS-23231	OVERDUE	[Security Issue S2] Oracle Java SE / Java SE Embedded Serialization Component Unspecified Remote Code Execution (CVE-2020-2604) - sbs-platform	OVERDUE	2020-03-19	Chuan-Sheng Chu
●	PSECBUGS-26896	OVERDUE	[Security Issue S2] Information Disclosure: Web Hosting	OVERDUE	2020-05-14	Tushar Gupta
●	SBSEC-836	OVERDUE	[Security Issue S1] ATS HTTP/2 DoS yinst package - small_business_services.US	OVERDUE	2020-05-15	Chuan-Sheng Chu
●	SBSEC-821	OVERDUE	[Security Issue Security-Task] YPHP EOL and Multiple Vulnerabilities - store.US	OVERDUE	2020-05-15	Chuan-Sheng Chu

Exiting Properties S-Bugs and EREs / S-Bugs Due in Next 7 Days by Organization

VERIZON LOCATION SERVICES	VGRID	SMALL BIZ
0	4	6

10 total issues — Issue Count by Organization

Exiting Properties S-Bugs and EREs / S-Bugs Due in Next 14 Days by Organization

VERIZON LOCATION SERVICES	VGRID	SMALL BIZ
0	17	8

25 total issues — Issue Count by Organization

Exiting Properties S-Bugs and EREs / S-Bugs Due in Next 30 Days by Organization

Outcome

We achieved over 90% security procedure adherence for external assets without direct control or authority.

After executing processes for escalation, consistently reporting status and metrics, and managing day to day operations, compliance ultimately increased by at least 50% and overall compliance improved to 90%+. Both companies involved were able to achieve cost avoidance by preventing legal action through better compliance. Improved reporting models and metrics to track open security vulnerabilities, program risks and issues, and high priority action items also ensured that executives had the ability to raise concerns early and ensure they were aligned with the program's status. In addition, after the program was mostly completed, team members within our client's cybersecurity department were trained on using reporting tools so that they could enable better risk management for future M&A activities that they anticipated would occur at the company in the future.

500+

Vulnerabilities tracked and remediated

100+

Compliance reports generated

WASHINGTON D.C.
(Headquarters)

8609 Westwood Center Dr., Suite 110,
Tysons Corner, VA 22182

CONTACT US

Christa Zubic, Senior Consultant
christa.zubic@dayblinkconsulting.com

DAYBLINK
CONSULTING

www.dayblinkconsulting.com