Managing Vendor Risks

State of North Carolina
2019 Annual Cyber Awareness Symposium
Vendor risk management is a key aspect of IT operations. Every organization should have processes in place to carefully assess and identify issues when considering using outsourced services.

- The challenges with current TPRM programs
- The art of the possible--what a perfect program might look like
- Data-centric assessments
- A day in the life of a risk analyst
- Whiteboard session--challenges, goals, dashboards
- Components of a solid TPRM program
- Optimizations to current operations
The Trouble with Third-Parties
Organizations are undergoing digital transformation to better deliver products and services to customers and drive innovation...

40% of all technology spending will go toward digital transformations*

$2T the amount enterprises will spend on digital transformations by 2019*

79% of organizations are adopting new technologies at a rate faster than they can address new security issues (Accenture)

*Source: IDC
Digital Transformation Expands Attack Surface

Companies continue to expand their digital ecosystem….

70% of organizations have “moderate” to “high” dependency on external organizations ¹

...Which poses new risks to the business

83% of organizations have experienced a third-party incident in the last three years ²

¹ Results from 2019 Deloitte survey
² Deloitte - EERM 2019 Survey
Risk is Growing, Actions Not Taken

65% rate their TPRM program as less than highly effective

64% of large organizations have no visibility into their third party environments

54% of organizations do not monitor the security and privacy practices of vendors

“2019 may be the year the Supply Chain Ecosystem, and concern about third party risk, officially hits the tipping point…”

- Kirstjen Nielson, Secretary of US Homeland Security @ RSA Conference 2018
Lack of Confidence in Current Approaches

**Existing Processes**

- Questionnaires
- Onsite assessments
- Penetration tests

**Current processes are valuable efforts to understand third party cyber risk but are not continuous, scalable, and staying ahead of this dynamic risk**

- “I know all the risk based on what my vendors tell me”
- “A single point-in-time view of risk is good enough”
- “I only need to focus on my top tier vendors - the others don’t matter”
Greatest Challenges

- Questionnaire Response/Validation
- Cross-functional Process
- Lack of Continuous Monitoring
- Assessments Take too Long
- Management and Executive...
- Third Party Inventory/Process Integration
- Third Party Issue Remediation
- Visibility into 4th Parties
- Influencing the Contracting Process
- Regulations/Standards
TPRM 2.0
Legacy TPRM Workflow

Board Reporting


www.bitsight.com
Continuous TPRM Workflow

Board Reporting


Periodic Timer

Risk Status Change
Continuous TPRM Workflow

Selection (RFP/x, M&A) → Assessment (Onboarding, Re-assessment) → Collaboration → Monitoring

Board Reporting

- Actions
  - EVA
  - Call
  - Reassessment
  - Onsite audit
  - Termination

Risk Status Change

Types of Security Program Evidence
- Questionnaire Responses (& artifacts)
- Certifications (ISO, SOC2, other audit)
- BitSight headline rating and risk vectors

Contract Terms
- Will monitor with SRS/BitSight
- Require interaction for observations
- Minimum standards
- Compel to work with BitSight on context

Workflow
- GRC
- Shared questionnaires
- EVA language
- etc.

Business Unit Need: Internal Questionnaire (inherent risk)
- Data sensitivity
- Systems access
- Business dependency
- Geographic reach

Tiering
Third Party Lifecycle

**INTEGRATION TO RISK SYSTEMS AND PROCESSES**
- GRC – leading indicators
- Issue Management
- Activity Plans
- API Integrations

**EVALUATION OF NEW VENDORS**
- Verification/Validation
- Evaluate Control Effectiveness

**FOCUS ON KEY VENDORS**
- Tiering by Criticality
- Recent incidents
- Trending down
- Drive 3 year resource plan
- Validate questionnaires
- Higher quality, data driven conversations

**INVESTIGATION**
- Celebrity Vulnerability e.g. ‘Bluekeep’
- 3rd and 4th party investigations

**OPERATIONS**
- Differentiated Alerting by Tier
- Management by exception
- Remediation and Enable Vendor Access

**BIT SIGHT PLATFORM**

**Risk Governance**

**On-Boarding**

**Continuous Assurance**

**Vendor Portfolio Management**

**Incident Investigation**

Proprietary & Confidential
© BitSight Technologies, Inc.
Data-Centric Risk Assessments
How BitSight Security Ratings are Calculated

BitSight Data Collection

Over 120+ data feeds
Including proprietary and exclusive data sources

The largest amount of proprietary data collection
BitSight collects 200+ Billion Events on a daily basis across 23 unique risk vectors

Exclusive data partnerships giving unprecedented visibility unavailable elsewhere
BitSight works with major ad networks, service providers and other unique data partners to provide visibility into organizational security posture unavailable elsewhere on the market.

Broadest Visibility into Emerging Areas of Cyber Risk
BitSight has visibility into emerging areas of cyber risk including Mobile Applications, Mobile Software, Internet of Things (IoT), File Sharing and more.
How BitSight Security Ratings are Calculated

Collect Data
200+ Billion events daily
Externally observable
World's largest sinkhole

Research & Assign
Automated & human validated
Public Internet registries
12+ month history for all companies

BitSight Digital Footprint Curation
Advanced Automated Mapping
Team of over 60+ technical researchers worldwide curating organizational
digital footprints

Broad Array of Sources
BitSight uses public registries, corporate documents, and technical
methods to determine the IP and domain footprint belonging to a company

Parent-Child Relationship Mapping
BitSight is the only security ratings provider with extensive parent-child
relationship mapping to ensure that corporate structure is properly
identified

Customizable Mappings of Your Organization
BitSight enables organizations to self-publish relevant ratings to the
BitSight platform for better risk visibility and communication. Examples
include regional breakouts (e.g. “France Operations”), excluding irrelevant
infrastructure like Guest Wifi (e.g. “Corporate Rating”) and more.
How BitSight Security Ratings are Calculated

Collect Data

200+ Billion events daily
Externally observable
World’s largest sinkhole

Research & Assign

Automated & human validated
Public Internet registries
12+ month history for all companies

Filter & Process

55% Compromised Systems
35% Diligence Information
10% User Behavior
Breaches when applicable

23 Risk Vectors

55% Compromised Systems
- Botnet Infections
- Spam Propagation
- Malware Servers
- Unsolicited Comms
- Potentially Exploited

35% Diligence Information
- SPF Domains
- DKIM Records
- SSL Certs/Config
- Open Ports
- Web Application Headers
- Patching Cadence
- Insecure Systems
- Server Software
- Desktop Software
- Mobile Software
- DNSSEC
- Mobile Application Security
- Domain Squatting

10% User Behavior
- File Sharing

Breaches if Applicable
How BitSight security ratings are calculated

**Collect Data**
200+ Billion events daily
Externally observable
World’s largest sinkhole

**Research & Assign**
Automated & human validated
Public Internet registries
12+ month history for all companies

**Filter & Process**
23 RISK VECTORS
55% Compromised Systems
35% Diligence Information
10% User Behavior
Breaches when applicable

**Calculate Rating**
Daily Ratings
Range from 250 to 900
Low ratings correlated to
higher likelihood of breach

120 DATA SOURCES
QUALIFIED DATA
200,000+ COMPANIES MAPPED
TESTED AND VALIDATED DATA
200,000+ COMPANIES MAPPED
PROCESSED DATA
SECURITY RATING
Strong, validated correlation to data breach

BitSight provides a **measurable range of risk** and is the only ratings solution with a **third party verified correlation to breaches**.

### Likelihood of suffering a data breach

If the security rating drops below 400 as compared to an organization with a 700 or higher*

<table>
<thead>
<tr>
<th>Security Rating</th>
<th>Likelihood of Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;400</td>
<td>x5</td>
</tr>
<tr>
<td>400-500</td>
<td>x4</td>
</tr>
<tr>
<td>500-600</td>
<td>x3</td>
</tr>
<tr>
<td>600-700</td>
<td>x2</td>
</tr>
<tr>
<td>&gt;700</td>
<td></td>
</tr>
</tbody>
</table>

*AIR Worldwide reviewed and approved our data and analyses

If 50% of computers run outdated Operating System versions**

If the **Botnet Grade** is **B or lower***

Or the **File Sharing grade** is **B or lower**

Or the **Open Ports grade** is **F**

**A Growing Risk Ignored: Critical Updates**

***Beware the Botnets: Botnets correlated to a higher Likelihood of a Significant Breach
A WEALTH OF DATA IS DRIVING NEW INSIGHTS

The insurance industry is gaining real-time insight into which companies are most vulnerable to cyber attacks—insight that can fuel intelligent growth.
**Goal:** Monitor the information security disposition of critical third party service providers

**Actions by BitSight**

- Monitor thousands of third parties
- Evaluate risk rating for each provider
- Determine risk areas for action

**Results**

- 6x Third party expansion coverage with same FT employees
Impactful Results from Vendor Collaboration

Onboarded **496** suppliers and engaged with BitSight Security Ratings as part of this process.

- **56%** saw a rating increase.
- Average points increased across this group by **276**.

* Suppliers on-boarded between May 1st and October 31. Ratings compared between May 1st and Dec 4th.
A Day in the Life of a Risk Analyst
The TPRM Maturity Continuum

Visibility

- Drill Down on Critical Risks
- Customize Alerts

Prioritization

- Focus on the Riskiest Issues
- Target Resources

Collaboration

- Take Action Based on Context
- Communicate Proactively
Executive Summary

• Prior to June 2018, at top of Industry Range
• 80 point drop due to configuration of external systems
• Can recover all points quickly

Vendors

• Vendors range from 480 to 760
• 1 public compromise, Acme PII exposed
• Reassess 3 vendors (partial / contextual)

Program Maturity

Identify
Situation awareness: assets, policies

Protect
Defensive controls and procedures

Detect
Automated and manual analysis of data

Respond
Mitigate technical and brand damage

Executive Summary

• Prior to June 2018, at top of Industry Range
• 80 point drop due to configuration of external systems
• Can recover all points quickly

Operational Excellence

Incidents
System compromises & data exposure

Diligence
Configuration, patching, & hardening

Executive Summary

• Vendors range from 480 to 760
• 1 public compromise, Acme PII exposed
• Reassess 3 vendors (partial / contextual)
Whiteboard Session

What are the challenges with your TPRM program?

What are your TPRM program goals?

What would be on your ideal executive dashboard?
Components of a Solid TPRM Program
Foundations, Assessments, Operations

**Foundations**
- Frameworks, Policies, & Process
  - Roles & Responsibilities
  - Governance & Program Sponsorship

**Assessments**
- Communication & Remediation
  - Risk Assessments
  - Vendor Inventory & Tiers

**Operations**
- Process & Improvement
  - Dashboards & Reporting
  - Continuous Monitoring
Stories from the Field: Roles & Responsibilities

• Case file:
  • Large company in the hospitality industry
  • 100s of third-parties: managing customers, managing properties, etc.
  • One IT administrator managed TPRM program as additional duty
  • New Director of Risk inherited a program that had:
    • No clearly defined mission
    • A skeleton budget and resources
    • No real metrics to report to management

• Lessons learned:
  • Symptom of lack of executive sponsorship
  • Tools alone don’t substitute for governance
Program Considerations

- Governance
  - Program Drivers
  - Sponsor
  - Cross-functional participants
- Assessment Process
  - From Business to Cyber
  - Questionnaires / Frameworks
  - Interviews / Onsite Assessments / Evidence Gathering
  - Tools – Current / Planned
- Population
  - Number of vendors and other third parties
  - Tiering / Third Party Criticality
Stories from the Field: Align with Business Goals

• Case file:
  • What are the risk goals of the organization?
  • Are they well known across all areas of risk management?
  • In many cases, operations believes their role is to limit liability, not necessarily to reduce risk

• Lessons learned:
  • Need a clear vision, align with these objectives
  • Get buy in with from stakeholders / points-of-interaction
    • Executive management
    • Procurement--Enterprise and operating units
    • Lines-of-business
    • IT risk / cybersecurity
Stories From the Field: Know Your Organization’s Personality

• Case file:
  • IT risk / cybersecurity only involved in vendor selection and assessment if LOB remembered
  • Sometimes procurement or legal flagged vendor, sometimes IT risk finds out about vendor after contract is signed
  • Culture of innovation, laissez-faire
• Lessons learned:
  • Culture can dictate decentralized decisions vs. top-down policy
  • Find the right checks and balances for your culture
Example Stakeholder Model (Medium Enterprise)
Example Stakeholder Model (Large Enterprise / Complex)
Stories From the Field: When in Doubt, Include IT Risk

- Case file
  - Well designed VRM and TPRM process
  - Strong support from management, central authority, published process
  - LOB ordered forklifts, which were not flagged as IT risks by LOB
  - Forklifts required IP addresses (everything is an IoT device), triggered late-stage cyber risk assessment

- Lessons learned
  - Involve IT Risk in all inherent risk assessment
  - Provide a feedback loop so vendor categories and goods/services are assigned a risk type that can be updated as products evolve
Stories from the Field: Stale Process

• Case file
  • Questionnaires rule, with SOC2, ISO, and other audit results / attestations by a nose
  • Lack of trust in actual data, which is more accurate and shows the ground truth
  • Fear of change, fear of becoming obsolete

• Lessons learned
  • Don’t be afraid to evolve your processes, that’s how you can optimize resources
  • There isn’t a trade-off between optimizing resources and reducing risk: you can have both
  • Plan for how to manage the message to existing staff; offer them enhanced roles
Improving Questionnaires
Questionnaires

Framework-based Assessments / Questionnaires

Pros

- Align with sources of best practice (ISO, NIST, etc.)
- Clarify elements of policy
- Review program components not visible externally

Cons

- Difficult to verify and validate responses
- Process can be time-consuming
- Only represent a point in time
Selecting the Right Questions

- A question should help to determine the existence of a control that mitigates risk
  - Data Breach or Loss
  - Spread of malware
  - Potential sabotage (i.e. network interruption, disrupt “the grid”)

- Consider limiting questions about Policies, Processes and Security Assessment Reports (i.e. SOC2)
  - Instead create a ”Document Collection List”
  - Assume if a document is not submitted, it does not exist
  - Documents are generally clues to the existence of a control, not a control that mitigates risk
Streamlining Current Questionnaires

- Eliminate redundant questions

16 Has the management established an information security awareness and training program? If yes, please describe.

18 Are employees and contractors required to complete a security awareness training? If yes, please list the topics covered and the frequency of the information security training program, and specifically highlight whether users are trained to identify and prevent phishing attempts?

- Eliminate overly granular questions

Program must ensure that the destruction of a key is witnessed by the key custodians with the appropriate records retained for audit purposes. Each key or key component destruction should record the following:
- The date and time of the keying material destruction
- The reason for destroying the keying material
- The full name and signature of the individual authorizing the destruction
- The full name and signature of the individual destroying the keying material, and
- The full name and signature of the persons witnessing the destruction.
Aligning Questions with Risk Vectors

<table>
<thead>
<tr>
<th>Diligence</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPF Domains</td>
<td>B</td>
</tr>
<tr>
<td>DKIM Records</td>
<td>B</td>
</tr>
<tr>
<td>TLS/SSL Certificates</td>
<td>C</td>
</tr>
<tr>
<td>TLS/SSL Configurations</td>
<td>C</td>
</tr>
<tr>
<td>Open Ports</td>
<td>B</td>
</tr>
<tr>
<td>Web Application Headers</td>
<td>F</td>
</tr>
<tr>
<td>Patching Cadence</td>
<td>F</td>
</tr>
<tr>
<td>Insecure Systems</td>
<td>A</td>
</tr>
<tr>
<td>Server Software</td>
<td>C</td>
</tr>
<tr>
<td>Desktop Software</td>
<td>C</td>
</tr>
<tr>
<td>Mobile Software</td>
<td>B</td>
</tr>
<tr>
<td>DNSSEC*</td>
<td>C</td>
</tr>
<tr>
<td>Mobile Application Security*</td>
<td>N/A</td>
</tr>
<tr>
<td>Domain Squatting **</td>
<td>N/A</td>
</tr>
</tbody>
</table>

- Email security
- Encryption
- Vulnerability management
- Patch Management
- Configuration Management
- Hardening standards

What evidence do you have about security program practices?
## Aligning Questions with Risk Vectors

<table>
<thead>
<tr>
<th>Diligence</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SPF Domains</td>
<td>B</td>
</tr>
<tr>
<td>DKIM Records</td>
<td>B</td>
</tr>
<tr>
<td>TLS/SSL Certificates</td>
<td>C</td>
</tr>
<tr>
<td><strong>TLS/SSL Configurations</strong></td>
<td>C</td>
</tr>
<tr>
<td>Open Ports</td>
<td>B</td>
</tr>
<tr>
<td>Web Application Headers</td>
<td>F</td>
</tr>
<tr>
<td>Patching Cadence</td>
<td>F</td>
</tr>
<tr>
<td>Insecure Systems</td>
<td>A</td>
</tr>
<tr>
<td>Server Software</td>
<td>C</td>
</tr>
<tr>
<td>Desktop Software</td>
<td>C</td>
</tr>
<tr>
<td><strong>Mobile Software</strong></td>
<td>B</td>
</tr>
<tr>
<td>Mobile Application Security</td>
<td>N/A</td>
</tr>
<tr>
<td>Domain Squatting **</td>
<td>N/A</td>
</tr>
</tbody>
</table>

- Perimeter security
- PCI Compliance
- Firewall Standards
- Mobile security
- Secure development
Aligning Questions with Risk Vectors

<table>
<thead>
<tr>
<th>Diligence</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPF Domains</td>
<td>B</td>
</tr>
<tr>
<td>DKIM Records</td>
<td>B</td>
</tr>
<tr>
<td>TLS/SSL Certificates</td>
<td>C</td>
</tr>
<tr>
<td>TLS/SSL Configurations</td>
<td>C</td>
</tr>
<tr>
<td>Open Ports</td>
<td>B</td>
</tr>
<tr>
<td>Web Application Headers</td>
<td>F</td>
</tr>
<tr>
<td>Patching Cadence</td>
<td>F</td>
</tr>
<tr>
<td>Insecure Systems</td>
<td>A</td>
</tr>
<tr>
<td>Server Software</td>
<td>C</td>
</tr>
<tr>
<td>Desktop Software</td>
<td>C</td>
</tr>
<tr>
<td>Mobile Software</td>
<td>B</td>
</tr>
<tr>
<td>Mobile Application Security</td>
<td>N/A</td>
</tr>
<tr>
<td>Domain Squatting</td>
<td>N/A</td>
</tr>
</tbody>
</table>

- Secure development (SDLC) / Web application security /
- [Sec]DevOps
- Encryption
- Config / change management
Aligning Questions with Risk Vectors

<table>
<thead>
<tr>
<th>Compromised Systems</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Botnet Infections</td>
<td>F</td>
</tr>
<tr>
<td>Spam Propagation</td>
<td>A</td>
</tr>
<tr>
<td>Malware Servers</td>
<td>A</td>
</tr>
<tr>
<td>Unsolicited Communications</td>
<td>A</td>
</tr>
<tr>
<td>Potentially Exploited</td>
<td>D</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User Behavior</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>File Sharing</td>
<td>A</td>
</tr>
</tbody>
</table>

- Endpoint protection
- Incident management / Detection and response
- Security awareness / training
### Aligning Questions with Risk Vectors

<table>
<thead>
<tr>
<th>User Behavior</th>
<th>Incident management</th>
<th>Data loss prevention</th>
<th>Secure disposal</th>
<th>Capacity management / BCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exposed Credentials **</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public Disclosures</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Breaches</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Disclosures *</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How It’s Done Today

Result: Significant assessment effort, some redundancy, burden on vendors, slow selection & onboarding
Modified Process: Less Effort, Less Risk

Security Ratings: Independent Observation
- Botnet Infections
- Malware Servers
- Spam Propagation
- Unsolicited Communications
- Potentially Exploited
- File Sharing
- Exposed Credentials
- Breaches
- SPF Domains
- DKIM Records
- TLS/SSL Certificates
- TLS/SSL Configurations
- Web Application Headers
- Open Ports
- Patching Cadence
- Server Software
- Desktop Software
- Mobile Software
- Mobile Application Security
- DNSSEC
- Domain Squatting

Artifacts: Self Aspiration
- Policy Statement
- Policy Process
- Policy Procedure

Audit Reports: Independent Review
- Control Audit 1
- Control Audit 2
- Control Audit 3

Questionnaire: Self Attestation
- Question 1
- Question 2
- Question 3
- Question 250
Modified Process: Less Effort, Less Risk

Security Ratings: Independent Observation
- Botnet Infections
- Malware Servers
- Spam Propagation
- Unsolicited Communications
- Potentially Exploited
- File Sharing
- Exposed Credentials
- Breaches
- SPF Domains
- DKIM Records
- TLS/SSL Certificates
- TLS/SSL Configurations
- Web Application Headers
- Open Ports
- Patching Cadence
- Server Software
- Desktop Software
- Mobile Software
- Mobile Application Security
- DNSSEC
- Domain squatting

Artifacts: Self Aspiration
- Policy Statement
- Policy Process
- Policy Procedure

Audit Reports: Independent

Questionnaire: Self Attestation
- Question 1
- Question 2
- Question 3
- Question 250
Modified Process: Less Effort, Less Risk
Modified Process: Less Effort, Less Risk

Security Ratings: Independent Observation
- Botnet Infections
- Malware Servers
- Spam Propagation
- Unsolicited Communications
- Potentially Exploited
- File Sharing
- Exposed Credentials
- Breaches
- SPF: Domains
- DKIM: Records
- TLS/SSL: Certificates
- TLS/SSL: Configurations
- Web Application Headers
- Open Ports
- Patching Cadence
- Server Software
- Desktop Software
- Mobile Software
- Mobile Application Security
- DNSSEC
- Domain Squatting

Artifacts: Self Aspiration
- Policy Statement
- Policy Process
- Policy Procedure

Questionnaire: Self Attestation
- Question 1
- Question 250
Modified Process: Less Effort, Less Risk

Result:
Reduced effort, little redundancy, minimal burden on vendors, speedy selection & onboarding
Tiering and Vendor Communication
Third Party Tiering

- **Business Risk**
  - Nature of Services and Industry
  - Geography
  - Financial Strength / Credit Worthiness

- **Data Criticality**
  - Data Classification – Confidential, Sensitive, Proprietary or similar
  - Sensitive Data Types – PII, Customer Data, Compliance, other protected data

- **Connectivity**
  - Direct connections to network
  - Indirect connections or access

Proprietary & Confidential © BitSight Technologies, Inc.
Vendor Communication

Leverage

...can we influence security improvements?

Context

...does it align with service the business uses?
Please note that the following does NOT constitute legal verbiage or advice from BitSight not any individual employed by or associated with BitSight.

<customer> will monitor <vendor> using a security rating system (SRS)

<vendor> will assign a point-of-contact for responding to inquires about the ratings observations.

<vendor> agrees to maintain a minimum rating and standards for each observation area (e.g., risk vectors), as follows: 650 or above for the overall rating, an A for Botnet Infections and File Sharing, and a B for Open Port and the remaining risk vectors that count toward the overall rating.

<vendor> agrees to investigate observations made by the SRS, explain the reasons for the observations, and cooperatively come up with an action plan to remedy negative observations.

<vendor> will work with the SRS platform to provide context, such as, but not limited to, breaking out assets that comprise the risk surface relevant to <customer>, tagging assets, and adding notes to observations.
An Engaged Community Adds Context

**Participants**

- **CUSTOMERS** - 1,700 TOTAL
  - 1,700 CUSTOMERS
  - 2,063 EVA RECIPIENTS
  - 100+ PARTNERS

**Actions**

- 5,541 EVAs Sent in the Last 12 Months
- 2,444 Self-Published Ratings
- 130,000+ Pieces of User Generated Content

**Outcomes**

- More vendors familiar with BitSight ratings for better collaboration
- Gain insights from your vendors to better prioritize follow up action
- Add context to communicate your security posture with customers, regulators, insurers
- Prioritize issues with more context than other ratings platforms
Process Optimization
## Optimizing Assessment Resources

<table>
<thead>
<tr>
<th>Initial Assessment / Onboarding</th>
<th>Tier 1</th>
<th>Tier 2</th>
<th>Tier 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rating &gt;= 750</td>
<td>AND Botnet = A</td>
<td>Partial questionnaire / assessment</td>
<td>Attestation (ISO, NIST, SOC)</td>
</tr>
<tr>
<td></td>
<td>AND Open Ports &gt; C</td>
<td></td>
<td>Onboard (no assessment)</td>
</tr>
<tr>
<td></td>
<td>AND File Sharing = A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AND Breach = A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rating 650-750</td>
<td></td>
<td>Full assessment</td>
<td>Partial assessment, focusing on gap areas</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Attestation (ISO, NIST, SOC)</td>
</tr>
<tr>
<td>Rating 500-650</td>
<td>OR Botnet &lt;= C</td>
<td>Onsite audit</td>
<td>EVA outreach, possible onsite audit</td>
</tr>
<tr>
<td></td>
<td>OR Open Ports = F</td>
<td></td>
<td>Full assessment and EVA outreach</td>
</tr>
<tr>
<td></td>
<td>OR File Sharing &lt;= C</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OR Breach &gt;= C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rating &lt; 500</td>
<td></td>
<td>Refuse vendor</td>
<td>Onsite audit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>EVA outreach</td>
</tr>
</tbody>
</table>
## Continuous Monitoring Action Matrix

<table>
<thead>
<tr>
<th>Continuous Monitoring / Reassessment Period</th>
<th>Tier 1</th>
<th>Tier 2</th>
<th>Tier 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rating &gt;= 750</td>
<td>Attestation (ISO, NIST, SOC)</td>
<td>No reassessment</td>
<td>No reassessment</td>
</tr>
<tr>
<td>Rating 650-750</td>
<td>Partial assessment, focusing on gap areas</td>
<td>Attestation (ISO, NIST, SOC)</td>
<td>No reassessment</td>
</tr>
<tr>
<td>Rating &lt;650</td>
<td>Onsite audit</td>
<td>EVA outreach, possible onsite audit</td>
<td>Partial assessment, focusing on gap areas</td>
</tr>
<tr>
<td>Botnet &lt;=B</td>
<td>EVA outreach</td>
<td>EVA outreach</td>
<td>EVA outreach</td>
</tr>
<tr>
<td>File Sharing &lt;=B</td>
<td>EVA outreach</td>
<td>EVA outreach</td>
<td>EVA outreach</td>
</tr>
<tr>
<td>Open Ports = F</td>
<td>EVA outreach</td>
<td>EVA outreach</td>
<td>EVA outreach</td>
</tr>
<tr>
<td>Data Breach &lt;C</td>
<td>Onsite audit</td>
<td>Onsite audit</td>
<td>Onsite audit</td>
</tr>
<tr>
<td>Data Breach A or B</td>
<td>EVA outreach</td>
<td>EVA outreach</td>
<td>EVA outreach</td>
</tr>
</tbody>
</table>

GRC tools, such as ServiceNow, and TPRM/VRM, such Whistic and Third Party Trust can automate and orchestrate risk management.
Customer Success that’s Part of Your Program

- Your Customer Success Manager is a strategic partner that accelerates your time-to-value with proactive engagement, from onboarding to operationalizing and beyond.
- Your Customer Success Manager is your trusted advocate to ensure you realize maximum value with BitSight. They will guide and advise you on the development of strategic and tactical roadmaps, understand your long and short-term needs, advise you on new product features and help you achieve your objectives.