Blueprint for Security Architecture & Strategy
DynTek Security Key Team Members

Joe Rubino
Vice President of Sales
joe.rubino@dyntek.com

Rob Costanza
Principal Architect, East Security Engineering
rob.costanza@dyntek.com

William Chang
Sr. IT Project Consultant Security Engineering
william.chang@dyntek.com

Steven Sanchez
Senior Account Executive
steve.sanchez@dyntek.com

Shaun Land
Principal Security Architect
CSO GHE & Commercial
shaun.land@dyntek.com

Steve Struthers
VP Security, CTO
steve.struthers@dyntek.com

Brian Zeno
District Sales Manager
brian.zeno@dyntek.com

Brett Harmon
Cyber Security Alliance Manager
brett.harmon@dyntek.com

Ron Ben-Yishay
CEO
ron.ben-yishay@dyntek.com
Representative Clients

HIGHER & K-12 EDUCATION
Representative Clients

FEDERAL, STATE & LOCAL GOVERNMENT
Representative Clients

HEALTHCARE

- HHC New York City Health and Hospitals Corporation
- Montefiore
  Inspired Medicine
- Adventist Health System
- Rochester Regional Health System
- Harvard Vanguard Medical Associates
  Atrius Health
- Reliant Medical Group
  Atrius Health
- VIDANT HEALTH
  "exceptional care, without exception"
- Harbor Health Services, Inc.

FINANCIAL

- PIMCO
- SSB State Street Bank
- First Foundation
  "Trust. Strength. Experience."
- Credit One Bank
- Credit Union of Southern California
  "Building Better Lives"
- CPS
- New York Life
Strategy Driven IT Security
Strategy

+ **Improves Results**
  Individuals always perform better when they know where they are going. Developing and publishing a Strategy for Security provides this.

+ **Reduces Complexity**
  A Security Architecture that is built as the result of a defined strategy simplifies the process of selecting the right people and technology.

+ **Improves Compliance**
  Auditors love details and checkboxes that are checked, but short of that, they appreciate strategy and a plan to get somewhere.

+ **Reduces Cost**
  A strategy allows you to build the detailed roadmap for improving security. When you know the long term plan, buying leverage goes up, as you can negotiate bundles and vendor investments.
The Process

- **Assess Current State and Goals**
  - Evaluate the existing client SOC, IT infrastructure, and core systems
  - Assess the health of the current state, and risks of the current deployment
  - Assess security control objectives
  - Be prepared to respond to OCR Audits and questions

- **Plan & Architect Future State**
  - Focus on optimizing existing investments
  - Identify alternatives and their associated costs
  - Develop a strategy and remediation/action plan

- **Remediate & Mature Current State**
  - Provide oversight of remediation plan for current controls to desired maturity and value

- **Deploy & Mature New Controls**
  - Provide oversight of implementation plan of new controls to desired maturity and value
1. What are the IT related RISKS to the organization?
   A. Which are IT security specific risks?

2. What are the options around managing/mitigating Risk (the Controls):
   A. People
   B. Process
   C. Technology

3. Prioritize the risks by Qualifying and Quantifying each.

4. Decide what you are NOT going to do (as an organization)

5. Create the Roadmap for what are ARE going to do.

6. Execute on the plan
Risk & Security Controls
Strategy, planning, implementation & operations
NIST Cyber Security Framework

Identify
- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

Protect
- Access Control
- Awareness and Training
- Data Security
- Info Protection Processes and Procedures
- Maintenance
- Protective Technology

Detect
- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

Respond
- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Recover
- Recovery Planning
- Improvements
- Communications
## Risk Management / Security Controls

### 59 Controls

<table>
<thead>
<tr>
<th>NETWORK PROTECTION</th>
<th>EMAIL / WEB</th>
<th>INCIDENT RESPONSE</th>
<th>DATA PROTECTION</th>
<th>RISK / COMPLIANCE</th>
<th>ENDPOINT PROTECTION</th>
<th>SERVER PROTECTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>Email Gateway</td>
<td>Network Visibility</td>
<td>Patch Management</td>
<td>Auditing / Monitoring</td>
<td>Anti-Virus / Anti-Malware</td>
<td>Anti-Virus / Anti-Malware</td>
</tr>
<tr>
<td>Intrusion Protection</td>
<td>Web Gateway</td>
<td>Endpoint Visibility</td>
<td>Database Security</td>
<td>Vulnerability Management</td>
<td>Disk Encryption</td>
<td>Advanced Anti-Malware</td>
</tr>
<tr>
<td>Behavioral Analysis Sandbox</td>
<td>Proxy</td>
<td>Forensics</td>
<td>Secure Backup</td>
<td>File Integrity Monitoring</td>
<td>Host IPS</td>
<td>Virtualization Security / Control</td>
</tr>
<tr>
<td>Network Application/Load Balancing</td>
<td>Email DLP</td>
<td>DLP Historical Analysis</td>
<td>Device Controls</td>
<td>Remediation Management</td>
<td>Desktop Firewall</td>
<td>Application Control / Whitelisting</td>
</tr>
<tr>
<td>Application Firewall</td>
<td>Web DLP</td>
<td>Adaptive Threat Protection</td>
<td>File Encryption</td>
<td>Log Management</td>
<td>Web Filter</td>
<td>Host DLP</td>
</tr>
<tr>
<td>Network DLP</td>
<td></td>
<td></td>
<td>DLP Data Location Classification, Access</td>
<td>SIEM</td>
<td>Mobile Data / USB Control / Encryption</td>
<td></td>
</tr>
<tr>
<td>Network Access Control</td>
<td></td>
<td></td>
<td>2 Factor Auth.</td>
<td>Risk Analysis Reporting</td>
<td>Application Control / Whitelisting</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SSL Certificate Management</td>
<td>DLP Reporting</td>
<td>Host DLP</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Password Vault</td>
<td>Network DLP</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Identity Access Management</td>
<td>Mobile Security Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Control Prioritization / Maturity Program

<table>
<thead>
<tr>
<th>NETWORK PROTECTION</th>
<th>EMAIL / WEB</th>
<th>INCIDENT RESPONSE</th>
<th>DATA PROTECTION</th>
<th>RISK / COMPLIANCE</th>
<th>ENDPOINT PROTECTION</th>
<th>SERVER PROTECTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>URL Filtering</td>
<td>Network Visibility</td>
<td>Patch Management</td>
<td>Log Management</td>
<td>Anti-Virus / Anti-Malware</td>
<td>Anti-Virus / Anti-Malware</td>
</tr>
<tr>
<td>Intrusion Prevention</td>
<td>(Required by Law CIPA)</td>
<td>Endpoint Visibility</td>
<td>Secure Backup</td>
<td>Policy Auditing / Monitoring</td>
<td>Web Filter</td>
<td>Advanced Anti-Malware</td>
</tr>
<tr>
<td>Secure Access Gateways</td>
<td></td>
<td>2 Factor Auth.</td>
<td>Device Controls</td>
<td>Vulnerability Management</td>
<td>Disk Encryption</td>
<td>Host IPS</td>
</tr>
<tr>
<td>Application Firewall</td>
<td>Email Gateway</td>
<td>Forensics</td>
<td>File Encryption</td>
<td>Identity Access Management</td>
<td>Advanced Anti-Malware</td>
<td>Virtualization Security / Control</td>
</tr>
<tr>
<td>Behavioral Analysis/Sandbox</td>
<td>Email DLP</td>
<td>Adaptive Threat Protection</td>
<td>2 Factor Auth.</td>
<td>SIEM</td>
<td>Network Access Control</td>
<td>Host IPS</td>
</tr>
<tr>
<td>Network Application/Load Balancing</td>
<td>Web DLP</td>
<td>DLP Historical Analysis</td>
<td>Database Security</td>
<td>DLP Data Location Classification, Access</td>
<td>Host DLP</td>
<td>Host DLP</td>
</tr>
<tr>
<td>Network DLP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Gartner Maturity Model

- **Level 1** – Initial
- **Level 2** – Developing
- **Level 3** – Defined
- **Level 4** – Managed
- **Level 5** – Optimal

- Firewall
- URL Filtering
- Network Visibility
- Patch Management
- Log Management
- Anti-Virus / Anti-Malware
- **Level 1** – Initial

- Intrusion Prevention
- Web Gateway
- Endpoint Visibility
- Secure Backup
- Policy Auditing / Monitoring
- Web Filter
- Advanced Anti-Malware
- **Level 2** – Developing

- Secure Access Gateways
- Email Gateway
- 2 Factor Auth.
- Device Controls
- Vulnerability Management
- Disk Encryption
- Host IPS
- **Level 2** – Developing

- Application Firewall
- Proxy
- Forensics
- File Encryption
- Identity Access Management
- Advanced Anti-Malware
- Virtualization Security / Control
- **Level 3** – Defined

- Network Access Control
- Email DLP
- Adaptive Threat Protection
- 2 Factor Auth.
- Change Control
- Mobility Security Management
- Application Control / Whitelisting
- **Level 3** – Defined

- Behavioral Analysis/Sandbox
- Web DLP
- DLP Historical Analysis
- Database Security
- DLP Data Location Classification, Access
- Network Access Control
- Host DLP
- **Level 4** – Managed

- Network Application/Load Balancing
- Network DLP
- SSL Certificate Management
- DLP Data Location Classification, Access
- DLP Reporting
- Host DLP
- **Level 5** – Optimal
# Example “Client Current State” View

<table>
<thead>
<tr>
<th>NETWORK PROTECTION</th>
<th>EMAIL / WEB</th>
<th>INCIDENT RESPONSE</th>
<th>DATA PROTECTION</th>
<th>RISK / COMPLIANCE</th>
<th>ENDPOINT PROTECTION</th>
<th>SERVER PROTECTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall 1</td>
<td>URL Filtering (Required by Law CIPA) 1</td>
<td>Network Visibility 1</td>
<td>Patch Management 1</td>
<td>Logo Management 1</td>
<td>Anti-Virus / Anti-Malware 1</td>
<td></td>
</tr>
<tr>
<td>Intrusion Protection 2</td>
<td>Web Gateway 2</td>
<td>Endpoint Visibility 2</td>
<td>Secure Backup 2</td>
<td>Policy Auditing / Monitoring 2</td>
<td>Web Filter 2</td>
<td></td>
</tr>
<tr>
<td>Secure Access Gateways 3</td>
<td>Email Gateway 3</td>
<td>Endpoint Threat Detection &amp; Response 3</td>
<td>2 Factor Auth. 3</td>
<td>Vulnerability Management 3</td>
<td>Advanced Anti-Malware 2</td>
<td></td>
</tr>
<tr>
<td>Application Firewall 4</td>
<td>Proxy 4</td>
<td>Forensics 4</td>
<td>Device Controls 4</td>
<td>Identity Access Management 4</td>
<td>Disk Encryption 3</td>
<td></td>
</tr>
<tr>
<td>Network Access Control 5</td>
<td>Email DLP 5</td>
<td>Adaptive Threat Protection 5</td>
<td>File Encryption 5</td>
<td>Change Control 5</td>
<td>Advanced Anti-Malware 4</td>
<td></td>
</tr>
<tr>
<td>Behavioral Analysis / Sandbox 6</td>
<td>Web DLP 6</td>
<td>DLP Historical Analysis 6</td>
<td>Database Security 6</td>
<td>SIEM 6</td>
<td>Mobility Security Management 5</td>
<td></td>
</tr>
<tr>
<td>Network Application / Load Balancing 7</td>
<td></td>
<td></td>
<td>SSL Certificate Management 7</td>
<td>Password Vault 7</td>
<td>Network Access Control 6</td>
<td></td>
</tr>
<tr>
<td>Network DLP 8</td>
<td></td>
<td></td>
<td>Collaboration Platform Security 8</td>
<td>Remediation Management 8</td>
<td>Host IPS 7</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Legend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Well Covered</td>
</tr>
<tr>
<td>Mostly Covered</td>
</tr>
<tr>
<td>Partially Covered</td>
</tr>
<tr>
<td>Not Deployed</td>
</tr>
</tbody>
</table>
## Healthcare “Client Future State” View

### Client Security/Risk Controls - ROADMAP

#### NETWORK PROTECTION
- **Firewall** 1
- **Intrusion Protection** 2
- **Secure Access Gateways** 3
- **Application Firewall** 4
- **Network Access Control** 5
- **Behavioral Analysis** Sandbox 6
  - **URL Filtering** (Required by Law CIPA) 1
  - **Email Gateway** 2
  - **Web Gateway** 3
  - **Proxy** 4
  - **Email DLP** 5
  - **Web DLP** 6

#### EMAIL / WEB
- **Web Filter** 2
- **Host IPS** 3
- **Application Control / Whitelisting** 5

#### INCIDENT RESPONSE
- **Network Visibility** 1
- **Endpoint Visibility** 2
- **Endpoint Threat Detection & Response** 3
- **Forensics** 4
- **DLP Historical Analysis** 5
- **Adaptive Threat Protection** 6

#### DATA PROTECTION
- **Patch Management** 1
- **Secure Backup** 2
- **2 Factor Auth.** 3
- **Device Controls** 4
- **File Encryption** 5
- **Database Security** 6
- **SSL Certificate Management** 7
- **Collaboration Platform Security** 8
- **DLP Data Location Classification, Access** 9

#### RISK / COMPLIANCE
- **Logo Management** 1
- **Policy Auditing / Monitoring** 2
- **Vulnerability Management** 3
- **Identity Access Management** 4
- **Change Control** 5
- **SIEM** 6
- **Password Vault** 7
- **Remediation Management** 8
- **File Integrity Monitoring** 9
- **Risk Analysis / Reporting** 10
- **DLP Reporting** 11

#### ENDPOINT PROTECTION
- **Anti-Virus / Anti-Malware** 1
- **Web Filter** 2
- **Disk Encryption** 3
- **Advanced Anti-Malware** 4
- **Mobility Security Management** 5
- **Network Access Control** 6
- **Host IPS** 7
- **Desktop Firewall** 8
- **Mobile Data / USB Control/ Encryption** 9
- **Application Control / Whitelisting** 10
- **Host DLP** 11

#### SERVER PROTECTION
- **Anti-Virus / Anti-Malware** 1
- **Advanced Anti-Malware** 2
- **Host IPS** 3
- **Virtualization Security / Control** 4
- **Application Control / Whitelisting** 5
- **Host DLP** 6

### Legend
- Optimize / Deploy Phase 1
- Deploy Phase 2
- Deploy Phase 3
- Do Not Deploy
- New Controls
Security Solutions

Success is …

- **40%** Product features and capabilities
- **30%** Deployment and maturity
- **30%** Administration and use/response
Getting the Organization Behind Security

*Making security the Organizations problem*

The organization typically looks at IT as the owner of the security problems (risks). Turning this around helps the rest of the organization become active “risk owners” and partners with IT.

**This is accomplished through:**

- Executive level risk messaging & education
- Improved Enterprise Risk Management (ERM) process
Executive Organizational Level Risk Messaging

Making your organization’s executive partners “security smart”

Simplify the "Risk Management Process" to common non-technical language, so that any executive can get it, own it and get behind it

- Take away the risk & security techno mumbo jumbo
- Use the risk & security controls graphic
- Educate the executive team on security through an “Executive Level Security Workshop” — they should be able to understand all the controls when you are done
- Leverage the Enterprise Risk Register
Improved Enterprise Risk Management Process

Getting the organization to own the Organizational Risks

IT’s job is to be in the RECOMMENDATION business:

• Identify risk (constantly and continuously)
• Analyze the risks
• Assign the risks (to an IT owner for tracking, and an executive decision maker (or team) to own the risk.
• Make recommendations for each risk to the organization (including prioritizing the risks)
• Executing on each risk as directed by the owner
• Tracking and managing known risks

The organizations job is to be in the RISK DECISION business:

• Contribute to the enterprise risk register
• Own the organizational risks
• Review the risks with IT
• Determine risk management for each risk (accept, remediate, reduce)
• Support IT with the risk decisions from the owners (budget, resources, time)
The Enterprise Risk Register

How it all happens – The IT View

<table>
<thead>
<tr>
<th>IT Security Enterprise Risk Register</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Assessment from Security Team</strong></td>
</tr>
<tr>
<td><strong>Risk Item Number</strong></td>
</tr>
<tr>
<td>23</td>
</tr>
</tbody>
</table>

**Recommended Risk Remediation from Security Team**

<table>
<thead>
<tr>
<th>Estimated Remediation Initial Cost</th>
<th>Estimated Initial Operational Cost (project professional services costs)</th>
<th>SFTE to Operate (100% = 1FTE)</th>
<th>Estimated Ongoing Operational Resource Costs (by SFTE required to operate &amp; maintain)</th>
<th>1st Year Remediation Costs (Capital and Resources)</th>
<th>Ongoing Costs (Year 2 &amp; X, OPEX and Resources)</th>
<th>Estimated Remediation Effort (Time / Duration)</th>
<th>Residual Risk (Post Remediation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$82,000</td>
<td>$66,000</td>
<td>30.00%</td>
<td>0</td>
<td>$45,000.00</td>
<td>$753,000</td>
<td>80 Days</td>
<td>Low</td>
</tr>
</tbody>
</table>

**Executive Business Risk Owner / Response**

<table>
<thead>
<tr>
<th>Risk Status</th>
<th>Assigned Executive Business Risk Owner (C-Level/Non-IT)</th>
<th>Risk Response Team Business Owner</th>
<th>Recommended Plan/Strategy</th>
<th>Response Plan Cost</th>
<th>Last Received Date</th>
<th>Days for Next Review</th>
<th>Days Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identified</td>
<td>Business Security Council</td>
<td>Remediate pursuant to Recommendations</td>
<td>Yes</td>
<td>Yes</td>
<td>7/1/2015</td>
<td>10/1/2015</td>
<td>0</td>
</tr>
</tbody>
</table>

This control will both harden the database environment, as well as automatically detect/prevent unauthorized and/or unusual activity in the database environment. This is critical for today’s threat landscape.
<table>
<thead>
<tr>
<th>Risk Item Number</th>
<th>Risk / Audit Finding Description</th>
<th>Current State (% Remediated)</th>
<th>Type of Risk</th>
<th>Risk Response Prioritization</th>
<th>Recommended Risk Remediation from Security Team</th>
<th>1st Year Remediation Costs (Capital and Resources)</th>
<th>Outdoor Costs (Year 2, 3, + OpEx and Resources)</th>
<th>Estimated Remediation Effort (Time / Duration)</th>
<th>Residual Risk (Post Remediation)</th>
<th>Next Steps Description</th>
<th>Risk Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>The organization cannot easily and automatically detect potential security and breach incidents within the database, as well as is unable to prevent them. When an attacker gets past all other security controls, data in databases is the primary target and databases are usually the warehouse for sensitive data.</td>
<td>0%</td>
<td>Business Operations, Reputation, Revenue</td>
<td>Very High</td>
<td>Cannot be remediated through people or process alone. To remediate this risk will require a database security solution. This control will both harden the database environment, as well as automatically detect/prevent unauthorized and/or unusual activity in the database environment. This is a critical control for today's threat landscape.</td>
<td>$155,000</td>
<td>$51,400</td>
<td>60 Days</td>
<td>Low</td>
<td>Approval from Business Risk Owner</td>
<td>Identified</td>
</tr>
<tr>
<td>24</td>
<td>The organization cannot easily and automatically detect potential security and breach incidents within the SharePoint environment, as well as is unable to prevent them. When an attacker gets past all other security controls, data is the target and SharePoint is a secondary warehouse for sensitive data.</td>
<td>0%</td>
<td>Business Operations, Reputations, Revenue</td>
<td>Very High</td>
<td>Cannot be remediated through people or process alone. To remediate this risk will require a SharePoint security solution. This control will both harden the SharePoint environment, as well as automatically detect/prevent unauthorized and/or unusual activity in the SharePoint environment. This is a critical control for today's threat landscape.</td>
<td>$93,000</td>
<td>$23,000</td>
<td>60 Days</td>
<td>Low</td>
<td>Approval from Business Risk Owner</td>
<td>Identified</td>
</tr>
<tr>
<td>25</td>
<td>The organization is at risk from data loss/shut from both physical and network-based threats. For example, an unencrypted tape drive with sensitive data could be lost or stolen and the data could be easily recovered from tape. Also, streaming data over the network for business can be a key point for someone purposefully looking to steal the data.</td>
<td>25%</td>
<td>Business Operations, Reputations, Revenue</td>
<td>High</td>
<td>Cannot be remediated through people or process alone. To remediate this risk will require a secure backup solution. Data is always a primary target. Encrypting data is critical, including backups of the data. This is a critical control for today's threat landscape. Some secure backups are taking place, but an enterprise solution needs to be deployed to all sites and used for all backup processes is a standardized manner.</td>
<td>$45,000</td>
<td>$445,000</td>
<td>30 Days</td>
<td>Low</td>
<td>Approval from Business Risk Owner</td>
<td>Identified</td>
</tr>
</tbody>
</table>
Security Services

• Over 40 experienced security consultants
• Services capability for architecture, deployment, support and staff augmentation
• Security Strategy Engagements
• PCI Readiness Engagements
• Cyber Attack Preparedness
• Breach / Incident Response Cyber Attack Response (like Ransomware)
  • PII/PHI Breach Response
  • Work with Incident Response partners like Cisco
• Vulnerability and Compromise Assessments
• Penetration Testing (yearly/periodically)
• Managed Security Services
Quick Facts

• DynTek’s security business growing 99% Y-o-Y (Q1 & Q2 2016 - grew 300%+)
• Cisco DVAR & Gold Partner
• Various Partner Awards such as Intel Partner of the Year 2016
• Locations across the US and more importantly people who can be onsite as needed
• We have a proven history of investing in key security segments for Commercial, Government, Healthcare, & Education
• Financing capability with flexible terms allowing you to leverage multi-year budgets without entering into a complex leasing agreement
Conclusion

We have developed a simplified model that IT executives and management can use to document and communicate the relationship between organizational risks and IT Security expenditures. The DynTek team is ready to assist in any aspect of improving your organizational security posture. From planning to design, to implementation and support, we look forward to the opportunity to assist.

What are the steps?
1. Identify the key strategies and associated risks.
2. Document and prioritize the risks based on IT’s understanding of the strategy.
3. Identify and select solutions to address each area of risk.
4. Present findings and recommendations to executive management for final determination.

A program that you continue to use, on a regular basis.
A Tradition of Partnering and Success!

McAfee Partner of the Year, Americas
Questions?