# APPLICATION RATIONALIZATION: A ROADMAP FOR IT SECURITY AND EFFICIENCY

***Authored by:***
*David Stone – Principal, Consulting Services, Divurgent*
*Quang Nguyen – Manager, Consulting Services, Divurgent*
*Saneel Vasram – Management Consultant, Gevity*

# INTRODUCTION

In May 2017, the National Health Service (NHS) in the United Kingdom was crippled by the global WannaCry ransomware attack, which was thought to have been created by a group tied to North Korea. As the crisis stretched into days, 40 hospitals were locked out of their IT systems, 16 were shut down, surgeries were canceled, and caregivers were forced to treat patients without access to their medical records, lab tests, x-rays, or even information on allergies. Physicians reverted to pen and paper to document care. During the shutdown, the attackers demanded ransom payments. The crisis only ended after Microsoft created a security patch that remedied the problem.

NHS had been warned over the year leading up to the attack that their systems were vulnerable to ransomware attacks. This was in large part because NHS organizations in the UK were using an untold number of systems and applications running on Windows XP, which was an outdated, 16-year-old operating system at the time (Bodkin, et. al., 2017).

Luckily, nobody died, but the attack was estimated to cost the NHS at least £19 million in lost output and £73 million in IT costs during and after the attack (Department of Health and Social Care, 2018).

It had been a growing information security disaster waiting to happen for at least a decade, but it did not have to be. If IT managers had conducted an effective application rationalization program prior to the attack, it likely never would have happened.

# WHAT IS APPLICATION RATIONALIZATION?

In business management, the word, “rationalization” usually refers to reorganizing a company in order to increase operating efficiencies, and it is a significant undertaking. Application rationalization is a rigorous process that occurs organization-wide in the IT space to identify which applications should be kept, replaced, retired, or consolidated toward that same goal of identifying risks and increasing efficiencies.

Application rationalization identifies opportunities to simplify the IT environment, reduce costs, and bridge the gaps among IT, business, and clinical areas. Unless the scope of the effort is clearly delineated at the beginning of the project, the process can quickly expand to include many of the following areas:

- Application Inventory
- Vendor Risk Management
- Portfolio Management
- Application Retirement
- Data Management
- Data Archival
- Policy and Procedure Review
- Contract Rationalization

Without a clear definition of the scope of the effort, strong governance, and an effective methodology this effort can quickly spin out of control. So, how did healthcare organizations get themselves into a mess that needs this much cleanup, what is the mess they are trying to clean up with application rationalization, and how bad can it be?

# HOW DID HEALTHCARE ORGANIZATIONS GET HERE?

The predicament that prompts the urgent need for applications rationalization is usually caused by one of three things:

1. Unfettered or unmanaged growth of the healthcare organization's information technology portfolio
2. Having been engaged in an aggressive mergers & acquisitions mode
3. A combination of both

***Unfettered and Unmanaged Growth***

The power structure within the health system has a huge impact on the ability of the IT organization to manage the application portfolio. Many organizations have, over time and with lax oversight, allowed the authorization for acquisition of IT assets to be decentralized. The result is often a hodge-podge of applications that are not subject to enterprise standards, monitoring or control. In response to this issue, an organization might attempt to create such standards on a centralized basis, but if there is no governance structure in place to enforce them, then the organization does not truly have effective standards, and growth of the application portfolio will continue unchecked.

The problem is, for example, that someone goes to a conference, sees a product and loves it, and as long as that person has a budget, he or she can buy the product and introduce it into the organization's application portfolio. This can create a multitude of problems, including whether the application will fit within the organization's infrastructure, and whether it will be able to pass data among other applications. Additionally, many examples arise where capital investment is considered, but little thought is given to ongoing operational costs such as licence renewal, version upgrades and other maintenance activities.

***Mergers & Acquisitions***

Mergers and acquisitions can also greatly contribute to difficulty in managing the application portfolio. Healthcare systems are rapidly acquiring physician practices and other hospitals. Each of those acquired entities will have its own application portfolio with varying or ineffective standards. The result is a complex IT environment with uncontrolled growth of the applications portfolio.

The requirement in healthcare to retain patient data also contributes to this problem. For example, a health system acquires a physician practice and requires the newly acquired practice to convert to the health system's standard ambulatory system. Now what are they going to do with all of that data that was collected using a different system? The application cannot be retired until the data is archived or otherwise made available. Unfortunately, health systems that acquire other healthcare organizations often do not, or are unable due to business conditions, to take into account how long it is going to take to integrate their IT, even though IT is critical to the operation of the health system.

The problem this causes is that IT organizations in healthcare end up spending more and more of their time and resources on maintenance, which does not give them the time and resources they need to innovate. An indication of how badly your healthcare organization may need application rationalization is the percentage of your IT department resources that are going into maintenance of the current portfolio and environment versus how much they have available for investment in new applications technology. For example, if your IT organization is at 80% maintenance and 20% new application investment or worse, you have major problems—redundancy, potential for breach exposure, conflicting security controls, ineffective or absent standards, and more. If yours is like most IT organizations in healthcare, management is constantly bombarding you with new projects they want you to work on, but you will never be able to innovate when you are using 80% of your resources maintaining your current application portfolio and infrastructure.

# TO DO APPLICATION RATIONALIZATION OR NOT – THE THREATS AND OPPORTUNITIES

The rationalization of applications can address many information security and information technology risks. First, let us address perhaps the most acute issue—information security (IS).

***Application Rationalization and Information Security***

Poor management of applications throughout the enterprise brings inherent IS risks. Here, we will take a look at half a dozen or so elements of an organization's potential IS exposure that application rationalization can identify and eventually remediate.

1. *Multiple vendors performing similar tasks using different security controls.* Let us say that in our organization we are using Vendor A's solution to do something at one site and then using Vendor B at another site, performing basically the same function, but each has different security controls. That means IT has to manage two different security control environments for the same function. Vendor A may be better than Vendor B, or vice versa. Either way, this security problem needs to be solved.
2. *Too many vendors to properly assess the risks to the organization.* A healthcare organization may have so many vendors that IT personnel cannot properly assess what the risks are to the organization. If the organization has two vendors instead of one for a particular function, and that pattern is replicated across the entire organization, you may have twice as many vendors as you need to support the organization. How can you stay on top of all of those vendors to make sure the security risks are being properly managed?

3. *Addition of new applications and vendors without a proper security risk assessment.* Another issue is that people are installing new applications and establishing new relationships with vendors without doing any proper risk assessment. Management needs to put something in place to ensure the risks associated with a vendor's solution is consistent with the organization's risk tolerance.
4. *Unsecured movement of data in and out of the organization.* Health systems are required to send data outside the organization all the time. If you have multiple applications and multiple vendors sending the same type of data, they may not be properly secured or they may be secured in different ways. There are substantial penalties associated with data breaches.
5. *Unsecured external access to the internal network.* Applications may be set up so they are maintained by an external entity. In the case of an acquired medical group, you might have a doctor who uses an application, but he or she does not know anything about managing this application, so they arrange for a vendor to come into the network and get on their application. This results in a vendor that may not have been vetted through IS standards having access to the internal network, resulting in a potential security exposure to business.
6. *Exposing internal security controls through outside facing applications.* If you have an application that people outside the organization are using, it can expose your internal security controls to the outside world. Knowing who is using those applications, how they are secured, and how they are being managed is important to the overall security of the organization.
7. *Effective management of access controls.* Managing access to applications is an important feature of an information security program. What applications do we have, where are they located, and how many people are using them?
8. *Inability of vendors to apply appropriate security patches.* Are your IT managers sure their vendors are updating the application products in your organization regularly to ensure their security? Some vendors are small companies, and they can't afford to keep their products running with the most up-to-date security patches and operating systems. That is why many health systems have applications based on outdated operating systems with security holes.

***Application Rationalization and Information Technology***

Beyond the issues of security, rationalization of applications can address many information technology and business-side concerns.

1. *Cost Reduction*
   a. Eliminate redundant applications and their associated costs
   b. Reduce and/or avoid infrastructure and operational costs by repurposing, resizing, and retiring infrastructure and system management from retired applications
   c. Reduce FTEs engaged in redundant support functions
   d. Reduce training costs by eliminating redundant applications
2. *Driving Standardization.* Application rationalization is one method for driving standardization across the organization, which reduces complexity andcost .
3. *Funding Innovation*. If your IT maintenance budget is continuing to grow exponentially, it is taking away from the innovation opportunity. Health systems always want to be innovating, improving, and reducing the costs of providing services to patients.

4. *Reduce the complexity of the IT environment.* One of the major goals of application rationalization is reducing the complexity of the IT environment, which makes IT standards easier to develop and enforce. It also provides opportunity to leverage data across the health system for intitavies such as business intelligence.
5. *Providing a greater understanding of the existing applications and inter-dependencies.* When the IT environment is less complex and there are fewer applications, it becomes easier to understand the inter-relationship and interdependencies of the applications.

***Application Rationalization and End Users***

So how does Application Rationalization affect the end users that IT serves?

1. Reduced complexity for end users. By reducing the number of applications that end users need to interact with on a daily basis, end users may benefit from a lower cognitive load so they can focus on their job and outcomes. This also reduces the cost of onboarding new staff, or transferring staff between departments.
2. Better customer support from IT. If IT has less applications they need to maintain, end users may benefit from higher quality and increased responsivess from support teams.
3. Increased IT responsiveness for new requests. Where IT personel are freed up to support a rationalized set of applications, more resources may be available to help with enhancements and/or innovative ideas.

# THE APPLICATION RATIONALIZATION PROCESS

Before we get into the application rationalization methodology, it is important to clarify some terms—specifically the difference between application rationalization and application portfolio management. Application rationalization is a project with a defined beginning and end. Application portfolio management is a continuous process that manages the life cycle of applications. Unless a portfolio management process is already in place, a portfolio management process is typically implemented during an application rationalization project.

Application rationalization is a large project that creates an application portfolio by taking an inventory of all applications in use across the organization and then examining the portfolio with the aim of reducing both the number of applications and number of vendors, thus reducing complexity. The process of rationalization (retiring, consolidating, replacing applications) can be time consuming.

Portions of the application rationalization process are typically done within other projects. For example, if you want to upgrade your endpoint operating system, you need to get a good inventory of what applications are running, so you can test to make sure the upgrades won't adversely affect the applications. The same goes for when you are planning to upgrade your server operating system.

You would also need to make sure you have an inventory of applications that are running on those servers, so that you can test them before you do the upgrades. In these cases, the inventory component of application rationalization would be a subset of the tasks within a larger project.

***Methodology***

At a high level, the application rationalization process consists of three steps: Planning and Identification, Rationalization Analysis, and Execution (see Figure 1). Initially, some elements of the first two process steps—Planning and Identification, and Rationalization Analysis—run in parallel. The Execution process step takes place once those previous process steps have been completed. All three of these steps are run in two tracks—the Application Track and the Process Track.

The Application Track addresses the current application portfolio and results in recommendations for the replacement, consolidation or retirement of applications. The Process Track addresses the policy and procedure issues that must be addressed to manage the application portfolio in the future. Figure 1 illustrates the key activities included in each step and track.

**Figure 1: Application Rationalization Process Steps and Tracks**

| Process Steps | Phase | Application Track | Process Track |
|---|---|---|---|
| Planning and Identification | Organize | Establish Project Governance<br>Finalize Project Scope<br>Finalize Project Plan<br>Finalize Project Staffing | |
| | Inventory | Select inventory tool<br>Identify deployed applications<br>Collect application metadata<br>Infrastructure and architecture | Identify existing policies<br>Identify existing proceedures<br>Collect existing documentation |
| Rationalization Analysis | Analyze | Finalize application assessment scheme<br>Finalize vendor assessment scheme<br>Define application categories<br>Perform application assessment | Identify Policy/Procedure Gaps<br>Update Policy/Procedures<br>Develop policy/procedures |
| | Roadmap | Define remediation approach<br>Identify dependencies<br>Develop timeline | Identify dependencies<br>Develop timeline |
| Execution | Remediation | Assemble remediation team<br>Develop detailed plans<br>Conduct vendor negotiations<br>Replace, retire, consolidate applications | Policy/Procedure Approval<br>Develop communications plan<br>Conduct training on new procedures |

*Planning and Identification*

The objective of the *Planning and Identification* process step (the first in the application rationalization process) is to establish the project direction (including scope, approach, and plan), and compile the applications and policy/procedure inventory.

Through interviews with key personnel, a Project Charter is developed and then presented to the project sponsor or governance group for approval. The Project Charter outlines the scope, objectives, and participants in the project.

This document also provides a preliminary delineation of roles and responsibilities within the organization, outlines the project objectives, identifies the main stakeholders, and defines the authority of the project manager. Client expectations for reporting frequency and decision-making processes are also established.

After approval of the Project Charter, detailed project and staffing schedules are developed and presented to the project sponsor or governance group for approval. Once the staff is in place, the development of the application and policy/procedure inventory begins.

Collection of the application inventory can be very labor intensive. Wherever possible, automated tools should be used to identify the locations and owners of applications. This process usually requires frequent meetings with application and process owners to gather the required data and documentation.

An automated tool should be used to create the initial documentation and maintain the information. A spreadsheet listing of applications, policies/procedures and supporting data has limited long-term value, and is not sufficient for ongoing management. Many helpdesk ticket systems have an asset management component that can be leveraged to meet this requirement. In some cases, a new inventory tool is selected and implemented.

The application data collected varies depending on the project objectives and the availability of the information. The following is a sample of the information that is typically collected for each application:

- General information
- Key IS and business contacts
- Business/clinical usage
- Decommissioning process
- Data retention requirements
- Infrastructure and architecture requirements
- Contracts and licensing
- Other information

Copies of any policies and procedure documentation are collected. High-level procedure descriptions are developed for any procedures for which no documentation exists.

*Rationalization Analysis*

The objectives of the Rationalization Analysis (the second step of the Application Rationalization process) is to define the criteria for assessing the applications, identify policy and procedure gaps, determine the disposition of each application, and develop a roadmap for implementation of the recommendations.

All policies and procedures are reviewed and compared against the information technology infrastructure library (ITIL) framework and established best practices for portfolio management and application risk assessment. Based on this review, detailed recommendations are developed for improving these processes. In some cases, sample policies and procedures are written and then provided to the project sponsor or governance group for approval.

The next step in the process is to develop criteria for assessing the identified applications. The criteria should take into account the current technical and application architecture, organizational concerns and risk tolerance and industry best practices. The recommended assessment criteria are then reviewed and approved by the project sponsor or governance group before the assessment process starts. **Appendix A** contains a sample of the criteria that could be used in these assessments.

Based on the policy/procedure review and the application assessment, a detailed roadmap is developed. This roadmap focuses on improving process, technical and functional quality, reducing annual support costs, eliminating redundancies, and filling possible gaps. The roadmap will identify:

- Short-term quick wins, most likely the retirement of low-value applications and implementation of new policies and procedures
- Mid-term objectives—typically applications that can be consolidated
- Long-term objectives, including applications that should be replaced

*Execution*

The last phase of the methodology implements the remediation recommendations contained in the roadmap. While the roadmap provides guidance on the disposition of applications, application dependencies, resource requirements and timing, there are still hard choices and organizational and cultural changes to be made within the organization.

The very first task is to implement the new portfolio management policies and procedures. Implementation of the roadmap recommendations will take time. Adherence to the portfolio management process will instill some discipline into the application acquisition process and reduce the risk of uncontrolled application growth. Senior leadership endorsement is crucial.

While many view application rationalization as a technical exercise, most of the work involves creating effective organizational change management. There have been many articles on change management, which will not be repeated here. However, the following are a few key organizational change success factors that should be given special attention as part of an application rationalization effort:

*Stakeholder Involvement*: In addition to the project team and the governance group, all the people who are affected by the application change need to be aligned with the overall vision and then actively engaged throughout the process.

*Shared Vision of the Future State:* Organizational culture is the commonly held attitudes, values, beliefs and behaviors of its employees. The culture of an organization is as unique and diverse as an individual's personality. If the employees of an organization believe that change is something to be feared and avoided, then change implementation is often reactive and haphazard. However, if the employees of an organization believe that change is worthwhile and is everyone's responsibility, then change and growth occur with relative ease. It is important that the roadmap be used to craft a positive view of the future.

*Communication*

The following are a few guidelines for the communication of the anticipated changes to the stakeholders:

- Use language appropriate to the audience and is the right balance between logic and emotion.
- Avoid using unnecessary jargon and buzz phrases.
- Make it clear to the stakeholders the change will impact their interaction with the application.
- To avoid incorrect rumors, provide stakeholders with a reliable and valid information source.
- Provide stakeholders with several communication channels where they can ask questions, voice concerns, and make recommendations.

*Training*

The impending application changes should have been stressed through frequent communication. It is now important to train the organization on any operational and procedural changes. A comprehensive training program can alleviate anxiety and encourage adoption of the new policies, procedures and operational support activities.

*Measurement of Progress*

Just implementing the identified application change is not enough to declare success. Meaningful metrics, which are consistent with the application change and measure the effectiveness of the change are needed.

***Methodology Deliverables***

The expected deliverables, subject to review and approval by the project sponsor or governance group, are:

- *Project management artifacts.* Standard PMBOK artefacts starting with a project charter defining the scope, timelines and governance of this initiative. Additional artefacts expected include a detailed project plan, stakeholder map, status reports, *etc.*
- *Application inventory.* The list of all applications in use, along with a series of fields for each to represent the metadata, metrics, assessment and categories determined at the start of the process. These fields to be documented may include:
    - Vendor, Application Name, Version(s), Application Type, Short Description, Cloud/OnPrem
    - Status, Date Procured, Contract End date, Product Age
    - Infrastructure
    - Recurring maintenance costs
    - Business and IT application owners, clients (departments), number of users
    - Support services and provisioning
    - Functional Category and subcategories
    - Prioritization Criteria and Assessment Ratings

- *Application risk assessment scheme/process.* A clear scoring scheme to help leadership and users score against a defined set of criteria each application. The assessment scheme is used to inform the future state roadmap by comparing the business value an application provides against the total cost of ownership. Depending on the scoring, applications will need to be retained, retired or replaced. The scoring categories and criteria need to be customized to the operating environments and strategic goals and may include categories such as:
    - Strategic Fit
    - Application and Information Architecture
    - Usage
    - Operational Support
    - Operational costs
    - Non-functional Considerations
- *Vendor risk assessment scheme/process.* a clear scoring scheme to help leadership and management determine the risk posed by current or future vendors and their mitigation strategies. Vendor risk management should then focus on high risk vendors to ensure appropriate mitigation of contractual, compliance, security or operational risks.
- *Portfolio management process. A* governance structure to help manage and maintain the application portfolio and developed inventory based on the ITIL framework. Importantly it will need to take into consideration the organization's strategic intent (such as mergers and acquisitions) to help manage application portfolio growth at the enterprise level. Items typically included are:
    - Governance Structure
    - Roles and Responsibilities (RACI)
    - Terms of References for each governance group.
    - Processes indicating key entry and escalation points.
    - Templates for process implementation (e.g., application intake/request form).
- *Updated/new policy and procedure documents.* Updated policies and procedures, endorsed by leadership, may need to be created or updated to cater for applications that are intended to remain. This is very much based on the outcome of the inventory and the strength of any existing portfolio management process. An example of such policies include disaster recovery, business continuity and operational support.
- *Roadmap detailing.* The future state roadmap will develop a high-level plan on which applications should be retained, retired or replaced and how that might occur within a specified timeline. The plan will need to be developed in conjunction with leadership to best align with strategy. It will also need to consider the change management challenges of implementing application portfolio management across existing sites, and any new sites that the organization intends to acquire.

*Project Team Structure*

This sample methodology assumes the following resources will be used during the project (see Figure 2). These may vary with the structure of different organizations. The next chart (Figure 3), shows the roles and responsibilities of these resources. The number and source of the resources varies based on the desired timeline and the client's desire to supply resources.

**Figure 2: Project Team Resources**

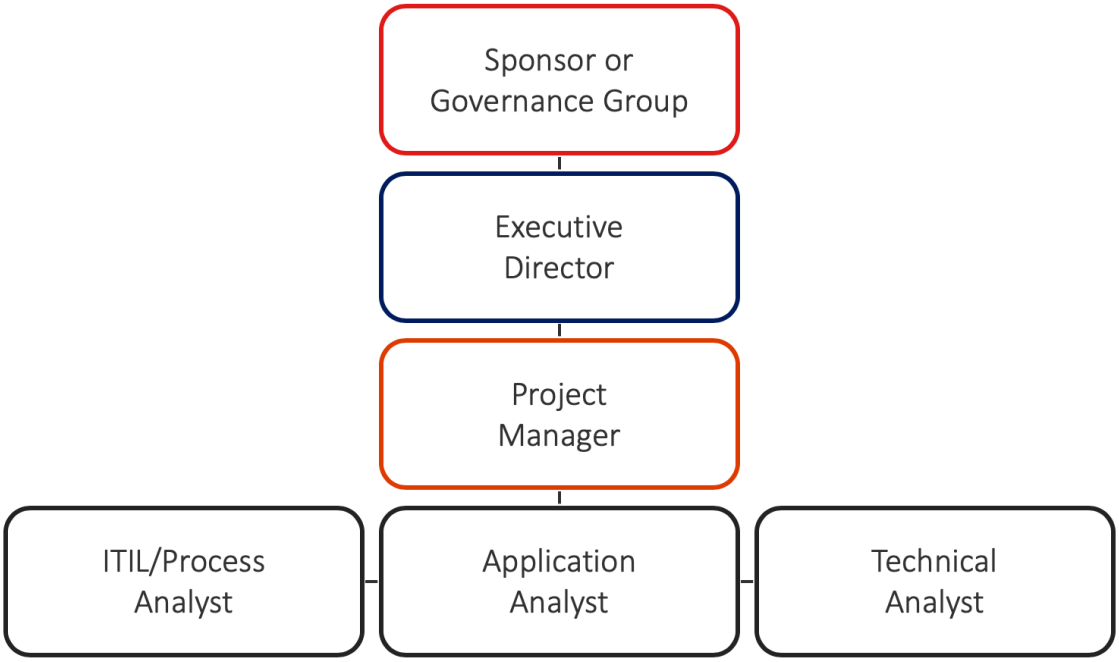


**Figure 3: Roles and Responsibilities of Team Resources**

| Role | Responsibility |
|---|---|
| Sponsor or Governance Group | Project Oversight<br>Key Decision Maker<br>Approve Project Deliverables |
| Executive Director | Quality of Project Deliverables<br>Liaison with Client Management<br>Communication with Steering Committee |
| Project Manager | Development of detailed Project Schedules<br>Management of Project Team<br>Status Reporting<br>Meeting Defined Milestones<br>Timely Issue Identification, Resolution, and Escalation<br>Development of Roadmap |
| ITIL/Process Analyst | Development of Policy and Procedure Inventory<br>Evaluation of Policies/Procedures against ITIL framework<br>Development of Policies/Procedure Recommendations |
| Application Analyst | Development of Application Inventory<br>Development of Application Assessment Process<br>Perform Application Assessment<br>Develop Application Recommendations |
| Technical Analyst | Use of Inventory and Application Scanning Tools<br>Assist in Application Assessments |

The project team will need access to select IT personnel and application owners during the application rationalization project. The specific resources and their expected time commitment must be identified and agreed to early in the project. The following are examples of tasks these resources may perform:

- Participating in the steering committee
- Identifying key business or clinical stakeholders to interview
- Providing the project team with access to the client IT environment and tools
- Running standard supply chain and accounting reports
- Explaining the business/clinical purpose of applications
- Describing current portfolio management and other related processes

# SUMMARY

Healthcare IT organizations face overwhelming challenges to gain operational efficiencies and reduce the complexity and cost of their application portfolio. A decentralized process for managing the application portfolio, sometimes caused by continued mergers and acquisitions, typically leads to organizational inefficiencies, redundant applications, higher IT costs and end user pain points. When 70-80% of the IT budget is needed to support aging low-value legacy applications and unnecessary application redundancies, it leaves insufficient resources left to invest in optimizing clinical and business processes through the use of information technology and supporting end users in efficienctly performing their roles.

Continuous improvement and realization of rationalization opportunities will help organizations reduce license costs, tap the existing portfolio's residual clinical/business value, and reduce functional overlap, all of which are key ingredients in an IT infrastructure that supports today's clinical/business requirements and anticipates tomorrow's needs.

# ABOUT THE AUTHORS

***David Stone – Principal, Consulting Services ,Divurgent***

As Principal, David leads Divurgent's strategic information technology and cybersecurity projects and a diverse portfolio in each area. With over 40 years of IT experience, over 20 of those years are in healthcare, David leverages his multi-industry experience to provide new perspectives on the use of information technology within a healthcare setting.

With expertise ranging from establishing IT organization from the ground up, optimizing EHR platforms, managing large-scale, complex technology projects, applying data-driven analytics, to leveraging clinical data to improve clinical processes and quality of care and establishing security processes, procedures, and policies.

David has held numerous positions including CIO, Information Security Officer, Program Manager, Project Manager, and Director of Applications, where he's been able to apply his years of dynamic experience in information technology and apply innovation solutions to today's top-of-mind IT challenges. When David is part of the consulting team, an organization gets more than just the knowledge and expertise to complete his assignment, they also get access to an experienced IT executive that can and will provide other value add expertise and guidance to the organization.

While David's healthcare experience spans multiple ambulatory and acute care settings, he has a strong focus in pediatric facilities.

***Quang Nguyen – Manager, Consulting Services, Divurgent***

In his role at Divurgent, Quang serves as a Consulting Services Manager focusing on change, problem and incident management optimization in an EHR setting. He primarily works with client Project Management Organization and Leadership committees that ensure their IT teams are using leading practice Information Technology Infrastructure Library methodologies. Quang is a firm believer in IT teams working with a singular strategy and standardization across all geographical and functional teams.

Quang has 13 years experience in hi-tech, manufacturing, legal IT and healthcare IT. His work includes helping clients in enterprise risk mitigation, security conguration, and leveraging system and data capabilities to mitigate risk. He has been in various roles such as infrastructure management, code / change management, documentation / segregation of duties and reporting tools development. He has with over 20 difference healthcare organizations in implementation, optimization and risk assessment projects.

***Saneel Vasram – Management Consultant, Gevity***

Saneel Vasram is a senior consultant with expertise in large scale, complex system design, development, delivery and operations. He facilitates an organization's ability to develop and execute strategic plans with a key focus on customer experience, using a combination of technical and non-technical solutions. Saneel has over 15 years of IT experience, with 8 of those in healthcare across Australia, Canada, Middle East, United Kingdom and the United States.

Saneel has expertise ranging from strategy development, enterprise architecture, people management, program and project management through to operational support. He is delivery focused, deeply empathetic about end-user experience, and passionate about healthcare and social service transformation.

# REFERENCES


1. *Bodkin H, et al. (2017, May 13). Government under pressure after NHS crippled in global cyber attack as weekend of chaos looms. The Telegraph. May 13, 2017.*
2. *Department of Health and Social Care (2018, October). Securing cyber resilience in health and care: Progress Update October 2018. Cyber Security Policy. October 2018.*


# APPENDIX A: SAMPLE ASSESSMENT CRITERIA

| | |
|---|---|
| 1 | Maintains an audit log for the location of all confidential data and their backups. |
| 2 | Has formal written information security policies. |
| 3 | Can provide results of a third-party external information security assessment conducted within the past 2 years. |
| 4 | Has a policy and procedure to protect client information against unauthorized access, whether stored, printed, spoken or transmitted. |
| 5 | Uses the following Information Security concepts: need to know, least privilege and checks and balances. |
| 6 | Implements AAA (Authentication, Authorization, Accounting) for all users. |
| 7 | Performs background checks for individuals handling confidential information. |
| 8 | Has termination or job transfer procedures that immediately protect unauthorized access to information. |
| 9 | Requires contractors, subcontractors, vendors, outsourcing ventures, or other external third-party contracts to comply with policies and customer agreements. |
| 10 | Has a policy that implements federal and state regulatory requirements. |
| 11 | Maintains a routine user information security awareness program. |
| 12 | Has a formal routine information security risk management program for risk assessments and risk management. |
| 13 | Implements network firewall protection. |
| 14 | Implements web application firewall protection. |
| 15 | Implements host firewall protection. |
| 16 | Provides network redundancy. |
| 17 | Uses enterprise virus protection on all systems. |
| 18 | Follows a program of enterprise security patch management. |
| 19 | Implements controls to restrict access to BSHSI data from other customers. |
| 20 | Ensures that remote access is only possible over secure connections. |
| 21 | Has managed, secure access points on its wireless network. |
| 22 | Implements encryption for confidential information being transmitted on external or Internet connections. |
| 23 | Implements encryption for confidential information at rest. |
| 24 | Changes or disables all vendor-supplied default passwords or similar “published” access codes for all installed operating systems, database management systems, network devices, application packages, and any other commercially produced IT products. |
| 25 | Ensures that passwords are never stored in clear text or are easily decipherable. |
| 26 | Implements redundancy or high availability for critical functions. |

| | |
|---|---|
| 27 | Sets the account lockout feature for successive failed logon attempts on all system's support computers. |
| 28 | Achieves individual accountability by assigning unique IDs and prohibiting password sharing. |
| 29 | Reviews access permissions for all server files, databases, application, etc. on a periodic basis. |
| 30 | Implements system event logging on all servers and records at a minimum who, what, and when for all transactions. |
| 31 | Reviews and removes dormant accounts on systems. |
| 32 | Monitors web server logs for possible intrusion attempts and significant changes in log file size as an indicator of compromise. |
| 33 | Reviews network and firewall logs. |
| 34 | Reviews wireless access logs. |
| 35 | Performs scanning for rogue access points. |
| 36 | Actively manages IDS/IPS systems. |
| 37 | Performs vulnerability scanning. |
| 38 | Performs penetration testing. |
| 39 | Checks routinely that password complexity is adhered to. |
| 40 | Has a written contingency plan for mission critical computing operations. |
| 41 | Has emergency procedures and responsibilities documented. |
| 42 | Stores backup media in a secure manner and controls access. |
| 43 | Maintains a disaster recovery plan. |
| 44 | Vendor's business associate contracts, or agreements, are in place and contain appropriate risk coverage for customer requirements. |
| 45 | Vendor's business associate agreements document the agreed transfer of customer's data when the relationship terminates. |