Bill of Health®

Security diagnostics and R_X for iSeries

iSeries security: why brick walls, padlocks, and powerful user footprint records aren't enough

It's a fact: many companies purchase a barrier product and/or a powerful user control tool and file their iSeries security concerns with the purchase order. Wish it were that simple, but it doesn't take a third-party incursion or a powerful IT user to threaten the security of data in your box.

Consider a household analogy with two-year-old twin girls: Brianamichelle and Kirsten.

Access control products lock down kitchen doors and tell you if one of the girls is jiggling a padlock. Powerful user authority products 'videotape' Brianamichelle's footprints if she somehow ends up in the kitchen all by herself while mom is responding to a Kirsten conniption upstairs.

The padlocks and the video camera provide scant comfort unless everything in the kitchen is so well configured that Brianamichelle could spend the whole day in there alone without any risk of hurting herself or burning the house down.

Unbeaten Path's Bill of Health software doesn't rely on the kitchen door lock or a footprint audit to protect the twins. Rather, it inspects access to and contents of each cabinet, appliance, chair, faucet, Wal-Mart bag, potted plant, and garbage can. Bill of Health then alerts you to configuration holes that one of the girls could wander into and makes a specific recommendation to close each hole.

iSeries security administrators that rely entirely on machine access barriers and/or powerful user footprint audits have an approach-avoidance attitude about becoming an operating system Ph.D. So, they buy barrier and/or footprint software and persuade themselves and auditors that the job is done. Well, the job isn't done.

Click **here** to see eye-opening illustrations of what can still go wrong (written in non-technical language).

An enormously complex subject

A patient student of i5/OS security administration will gradually learn that it is enormously complex. The security comes in categories of elaborate layers. Unless each facet is applied thoroughly and consistently, the integrity of the final result will have some unintentional vulnerabilities.

The good news is that a truly expert configuration will yield a comprehensive security lockdown. However, even well-informed, diligent security administrators are prone to overlook a few subtle details that end up compromising the quality of the final security result ... often in surprisingly significant respects. Said another way: **the size of the accidental security hole is frequently way out of proportion to the modest character of the oversight.**

Maybe i5/OS should be called 'iDiot mittens'

A well-intentioned security setting diligently applied to a single layer in category A of the operating system can unintentionally introduce a vulnerability in category B. That brings to mind a very funny story told by comedian Bill Cosby in the late '60s:

> Early in primary school Cosby kept losing his gloves. So, his mom equipped him with mittens that were connected with a cord that ran up one sleeve of his jacket and down the other. In the story, he called them **'idiot mittens'** because whenever he took a swing at a provocateur with his right hand he'd end up crunching the left side of his face with his other hand.

The ephemeral value of humor

The idiot mitten humor gets threadbare fast if you're a CIO confronted by these kinds of scenarios:

- A $350/hour Sarbanes-Oxley auditor shows up and takes three weeks to pick through all your OS/400 security settings. Once or twice a day the auditor sees you at the coffee pot and relates still one more subtle security vulnerability that he/she just discovered. Then the auditor prepares an 88-page PowerPoint "executive overview" presentation and takes all afternoon to present it to you and your boss. Wonderful.
- You are summoned to the CEO's office where you find her in a tense meeting with the traffic manager, the director of logistics, and the customer service manager. They all want to know how truckloads of your company's manufactured finished goods could have possibly been delivered at the CEO's summer cottage. High-priority customer master file investigation reveals that someone has tampered with ship-to addresses. Wonderful.
- You're pitching the proposed iSeries lease contract in the legal department when the General Counsel's assistant interrupts carrying a FAX. It's a copy of a letter distributed to an unknown number of your insurance customers signed by a programmer you terminated. The letter explains why their private health care data is not secure because HIPAA technical safeguards haven't been fully implemented by your company's IS department. Wonderful.

If something akin to these scenarios could happen at your enterprise, then a Bill of Health iSeries risk assessment would be a terrific idea ... the sooner the better. Once a Bill of Health Security Diagnostics report arrives in the hands of a CIO, he/she will be fully equipped to forestall the kind of disheartening scenarios presented above.

Bill of Health in a nutshell

Bill of Health runs a fine tooth comb through operating system security vulnerabilities and threats. The product then composes very comprehensive documentation about the risks that have been discovered and the potential security implications of each discovery. The diagnostics report is a Ph.D.-level description of distinctions between world-class security practice and a company's existing operating system configuration.

Bill of Health also prescribes an approach to mitigate all discovered risks within the context of security best practices ... think of it as "Cliff's Notes" for your iSeries security administrator.

Bill of Health should not be viewed as competitive with access denial and powerful user control/audit products. If you buy Bill of Health and use it well, the other products are probably not needed to secure your box. If you have purchased or intend to purchase the other products, Bill of Health is still an essential idea.

How to use Bill of Health

By following the steps below, your company will earn high value rewards from an investment in Bill of Health software:

The objective: Achieve and sustain a **clean** Bill of Health Security Diagnostics report.

The strategy: Investigate and mitigate any risks pointed out by Bill of Health reports. Then, use Bill of Health periodically to make sure that security threats are still screwed to the floor. Run the security diagnostics report each month ... plus ...

> ... run it after new software has been added, after significant application software modifications have been put into production, after IT staff turnover, after service providers have been on your iSeries, after changing a key communications supplier, and after changing physical access to your facility.

Save all the Bill of Health Security Diagnostics reports together with your internal notes on risk mitigation steps initiated.

The payoff: A sequence of **clean** Bill of Health Security Diagnostics reports would constitute compelling evidence of due diligence attention to iSeries security.

Sarbanes-Oxley auditors will be *very* impressed ... but they might also be disappointed because your portfolio of Bill of Health reports will remove +/-100 billable keyboard hours from their next SOX audit engagement.

Intellectual property digestible by non-technical staff

If you are the IT security administrator and you want to give your non-technical manager insight about how challenging your responsibilities are, please bring this **eye-chart presentation** to his/her attention. That page is an index to a wealth of intellectual property about operating system vulnerabilities. The content is written in plain English and it's peppered with a generous number of understandable illustrations.

Sample Bill of Health Security Diagnostics report

Even the most savvy iSeries professional will learn new things about operating system security by studying this Bill of Health Security Diagnostics report. This **sample deliverable** was automatically generated by Bill of Health software after analyzing the OS/400 configurations for a real iSeries at a company with this make-believe name: Vulnerabilities, Ltd.

IT departments that elect not to acquire Bill of Health will eventually end up creating this kind of documentation on their own. That brave initiative would begin with an exceptionally tedious learning curve and then graduate to an equally tedious one-command-line-entry-at-a-time process.

> It could take weeks to accomplish this. Then, after the report was completed, you'd be disappointed because it would not be accepted by SOX auditors. They have been required by PCAOB (sometimes pronounced 'peek-a-boo') to accept compliance evidence only if it has been generated by individuals with a high degree of objectivity. Your IT employees won't fit that profile.

up a notch™ security monitoring/remediation services

Unbeaten Path would be privileged to support your enterprise with these professional services:

- **Managed Security Services** monthly security monitoring reports
- **Remediating IBM iSeries operating system vulnerabilities**
- **Regulatory compliance vulnerability assessment and mitigation**

  Here's a copy of a **sample deliverable** from one of our security vulnerability assessment engagements (with a well disguised company ID).

Policy Minder software: compliance enforcement

Policy Minder software permits you to "freeze" your i5 operating system settings once you are confident all security risks have been remediated. At any future time, you can run **Policy Minder** to compare current security settings vis-à-vis the settings that were officially approved on an earlier date. The product has tools that permit QSECOFR to re-set anything that has moved back to the corporate policy. It's a powerful tool that even permits you to "transplant" your i5 security settings to a different instance of the operating system (e.g. a high availability box).

The compliance alphabet soup

Bill of Health Security Diagnostics reports comply with the most stringent requirements for risk assessments, vulnerability analyses, and IT security control due diligence described by the Information Systems Audit & Control Association (**COBIT**), the Food & Drug Administration (**21 CFR Part 11**), the **Sarbanes-Oxley** Act/**PCAOB** Accounting Standards No. 2, the National Institute of Standards & Technology (**NIST 800-30**), the Gramm-Leach-Bliley Financial Modernization Act (**GLBA**), and the Health Insurance Portability & Accountability Act (**HIPAA**).

Click **here** to see an index to overview information about the alphabet soup of standards, acts of Congress, and professional guidelines for IT security.

Questions ?

It would be a privilege to answer any technical questions about **Bill of Health** software. Here's Unbeaten Path International's contact information:

Toll free North America: (888) 874-8008
International: (+USA) 262-681-3151
Send us an e-mail (click **here**)

Unbeaten Path®