PUTTING THE HUMAN IN HIPAA:

GreyCastle Security Guides Oswego Health through its Annual Risk Assessment

- 1,200 EMPLOYEES
- 164 BEDS
- 17 LOCATIONS
- 24X7 CONTINUITY OF CARE

GreyCastle security

75% **of companies that experience a security breach have one thing in common: they hadn't performed a risk assessment properly or at all.**

Healthcare institutions around the world have become somewhat of a sitting duck for cyber attackers to pounce. With the amount of sensitive, personally identifiable data at stake, risk management in healthcare is a shared responsibility of increasing importance. After all, the "bad guys" only have to get one thing right, one time —while the "good guys" have to get everything right, every time.

When long-time customer, Oswego Health, came up on their annual HIPAA risk assessment requirement, they looked to GreyCastle Security to lead them through the process.

THE RESULTS

- A risk register identifying current gaps, threats, and vulnerabilities across the distributed healthcare network.
- A full-court-press approach to prioritizing each risk by impact to the organization at large.
- A corrective action plan designed to help Oswego Health meet compliance regulations while maturing its information security posture overall.

HERE'S HOW IT ALL WENT DOWN

BUILDING THE FOUNDATION

Over the past three years, Oswego Health CIO Barry Ryle, has worked alongside the team at GreyCastle Security to build their information security program from the ground up. **"We've reached out to GreyCastle Security for certain things that we either didn't have the expertise on-staff for, or things that we didn't have the time to do. They've been able to move those things forward—for us and with us—to help get Oswego Health to a better place."**

While this was hardly their first HIPAA risk assessment together, both teams viewed the process as a welcome opportunity to revisit Oswego Health's security controls with eyes wide open after a year that has been anything but ordinary. As the pandemic swept around the globe putting physical health under a microscope, derivative services like telemedicine placed added pressures on IT network health.

Any change to the business—whether it's a new partnership, a new technology or service, or even a new process—introduces risk from a cyber perspective. This is why GreyCastle Security takes the HIPAA risk management methodology and applies it on a continual basis with clients like Oswego Health, helping them move into a more strategic and proactive state. **"This means they're not making any decisions without understanding the full implications from a clinical, legal, financial, and reputational risk standpoint," notes Dan Didier, the Vice President of Solutions and Product Management for GreyCastle Security.**

STEP 1
ASSESS THE RISK

GreyCastle Security begins any HIPAA Risk Assessment by conducting a series of interviews with a cross-section of the organization. The goal is to gain full representation across all lines and levels of the business to understand where processes align and where gaps or vulnerabilities may exist.

"A lot of times our clients say to us, 'we don't know what we don't know'. And part of the risk assessment is to identify those things that you didn't know," shared Jillane Vennera, Account Manager at GreyCastle Security.

Through the HIPAA Security Law, highly regulated healthcare institutions like Oswego Health must perform this annual assessment in order to demonstrate compliance with a set of pre-defined security controls. And for some, the requirement stops there. Did we check the box—yes or no?

For Oswego Health, the assessment was a checkpoint to gauge success of current efforts and uncover opportunities for fine-tuning.

"We get a scorecard every year so we can see which areas we've improved on and which ones need to be strengthened."

Barry Ryle, Oswego Health CIO

STEP 2
PRIORITIZE BY IMPACT

After the initial interviews are held and the information synthesized, GreyCastle Security hosts a collaborative Risk Workshop with key organizational stakeholders to review and discuss the findings. Typically, this will include members from IT, HR, Legal, Finance, and the C-Suite. Here, each risk is prioritized based on its level of perceived impact to the organization. This allows the team to ask questions, talk through different scenarios, and create a prioritized corrective action plan together.

"If GreyCastle Security raises a concern, they're able to tell us why it's a problem and how to address it. They help us understand the issue in a way that we can communicate it to our staff, customers, and leadership," says Ryle. "It's having that expertise at your fingertips that you can call upon any time of day that goes such a long way."

"We bring a human approach to what's looked at as a very technical issue, wrongfully so, in many scenarios," says Didier. "At the end of it, we bring awareness not just to the folks in IT, but to the business as a whole. This gets them aligned so they can have meaningful conversations that go beyond bits and bytes, ones and zeros, and three-level acronyms. It's elevated from a technical to a business-level conversation."

STEP 3
CREATE THE ACTION PLAN

After the risk report is prioritized, both teams work to develop the mitigation plan in a highly collaborative process. “They don’t come in and say, ‘here’s everything that’s wrong, now go fix it,” says Ryle. “They help us figure out the best way to approach it within the structure of our organization.”

One example of an area the team identified as a need was to rework Oswego Health’s security policies and align them to regulatory compliance standards like NIST. “In the security world, if it isn’t documented, it never happened,” jokes Ryle. “On the other hand, you don’t want to create a policy that just sits around that no one uses or understands. So, GreyCastle Security helped us streamline and formalize our procedures and now they’re much easier for the team to reference, understand, and maintain.”

STEP 4
DEMONSTRATE PROGRESS

"We've been working with GreyCastle Security long enough that they're learning our environment more and more, so they truly are partners to us," Ryle continues.

> ***"These are not just people who come in, do a job, and leave. They're partners for the long-term."***
>
> **Barry Ryle,** Oswego Health CIO

It's good to know that you've got someone there who is helping mitigate or prevent a breach from happening. Oswego Health takes security very seriously and that's one of the reasons we've hired the best—and I do consider them one of the best. We wanted to work with a security company where security is all that they do because we're entrusted with very sensitive patient information. This is serious, so you want the best. That's why we're working with GreyCastle Security and working so feverishly to take our information security program to the next level."

ABOUT OSWEGO HEALTH

The mission of Oswego Health is to provide accessible, quality care and improve the health of residents throughout Oswego County. As a not-for-profit healthcare system that was established in 1881, Oswego Health is proud to continue to be one of Oswego County's largest employers. More than 1,200 employees work for the Oswego Health system, which includes the 132-bed community Oswego Hospital, a 32-bed psychiatric acute-care facility with multiple outpatient behavioral health service locations, The Manor at Seneca Hill, a 120-bed skilled nursing facility, and Springside at Seneca Hill, a retirement community. Oswego Health also has Health Services Centers located throughout Oswego County.

For more information about Oswego Health, please visit our website **www.oswegohealth.org**.

ABOUT GREYCASTLE SECURITY

GreyCastle Security was founded almost a decade ago on the principle that cybersecurity and effective defense is entirely possible if you use common sense, apply a system of measurement and know what you're trying to protect.

We help organizations to develop effective cybersecurity programs, minimize the impact of state and federal compliance regulations, improve client retention, and mitigate security incidents. Our revolutionary approach to service delivery solidifies the business mindset that cybersecurity is not just an "IT" issue – it's about the overall health of your business.

For more information, visit **www.greycastlesecurity.com**.